BENJAMIN C. MIZER
Principal Deputy Attorney General
ANTHONY J. COPPOLINO
Deputy Branch Director
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) 353-4556
Facsimile: (202) 616-8460
E-mail: kieran.g.gostin@usdoj.gov

Attorneys for Federal 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)(KAW)

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

Hearing Date: December 8, 2016
Time: 1:30 PM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules & Regulations

Other Authorities

NOTICE OF MOTION FOR SUMMARY JUDGMENT

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT on December 8, 2016, 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 for summary judgment, pursuant to Federal Rules of Civil Procedure 56(c), on all of the claims presented by Plaintiffs in this case. Pursuant to the Parties' Joint Case Management Statement, ECF No. 110, the Court has entered the following briefing schedule: Plaintiffs' Opposition and Cross-Motion shall be due on September 22, 2016; Defendants' Opposition and Reply shall be due on October 20, 2016; and Plaintiffs' Reply shall be due on November 17, 2016. ECF No. 112.

INTRODUCTION

The Nationwide Suspicious Activity Reporting Initiative (NSI) is a collaborative effort between federal, state, local, tribal, and territorial law enforcement related to the sharing of Suspicious Activity Reports (SARs) across jurisdictional lines. It seeks to build upon the longstanding practice by law enforcement of gathering tips and leads about suspicious activities, recording those tips and leads in SARs, and sharing that information (as appropriate) with other law enforcement entities. In order to better allow law enforcement agencies to identify and prevent future acts of terrorism, the federal government has sought to facilitate the sharing of useful SAR information—both by providing the technological means for law enforcement entities to share information with one another and by providing guidance intended to standardize the sharing process. Among other things, the Program Manager for the Information Sharing Environment (PM-ISE), pursuant to its statutory responsibilities under Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, codified as amended at 6 U.S.C. § 485, has issued the Functional Standard for the Information Sharing Environment, Suspicious Activity Reporting (Functional Standard).

Plaintiffs, five individuals who allege that SARs referencing them were shared among law enforcement entities in connection with the NSI, have brought a challenge to the lawfulness of that guidance. In particular, Plaintiffs challenge the Functional Standard's "reasonably indicative" operational concept, which instructs NSI participants that SARs should be shared through the NSI when they reflect "observed behavior" that is "reasonably indicative of pre-operational planning associated with terrorism or other criminal activity." Because the Functional Standard (including the "reasonably indicative" operational concept) is consistent with constitutional requirements, Plaintiffs do not assert claims under the First or Fourth Amendments, or any other constitutional provision. Instead, they assert that the PM-ISE's issuance of the Functional Standard is inconsistent with the Administrative

Procedure Act (APA). But Plaintiffs' claims ask too much of that statute—which imposes limited procedural requirements on federal agencies.

Plaintiffs' first claim asserts that the Functional Standard should be vacated because it was issued without the PM-ISE observing the APA's notice-and-comment requirements. 5 U.S.C. §§ 553(b)–(c). These requirements, however, only apply when an agency acts pursuant to its legislative authority, delegated by Congress, to issue rules that have the same force and effect as statutory enactments. While the PM-ISE does have such legislative authority, the language and structure of the Functional Standard make clear that it has not acted pursuant to that authority in connection with NSI. Instead, the PM-ISE has sought to develop the NSI through a collaborative process that seeks to find consensus among NSI participants regarding the best practices for sharing SARs. Consistent with that approach, the PM-ISE issued the Functional Standard as general policy guidance describing those best practices, rather than as a legislative rule that it could enforce through administrative (or judicial) proceedings against NSI participants.

Moreover, even if the PM-ISE had been required to observe the APA's notice-and-comment requirements when it issued the Functional Standard, any failure to comply with those technical requirements would have been harmless. The Functional Standard, as noted, has been developed over the past ten years through a collaborative process that involved both NSI participants and other interested parties. The advocacy organization that represents Plaintiffs, in fact, was heavily involved in the development of the current Functional Standard and, during that process, raised the very same concerns it raises in this lawsuit. The purpose of the APA's notice-and-comment requirements is to provide interested parties notice of proposed agency rules, an opportunity to comment on those rules, and a concise response to any comments raised. That occurred here, and remanding this matter to the PM-ISE to comply with the APA's technical procedural requirements would therefore achieve little more than imposing additional burdens and costs that would

be duplicative of the prior collaborative process. The APA does not contemplate the granting of relief in these circumstances.

Plaintiffs' second claim asserts that the PM-ISE's adoption of the "reasonably indicative" operational concept rather than the "reasonable suspicion" standard articulated in another federal regulation, 28 C.F.R. Part 23, is contrary to the APA's substantive requirements for agency decision-making, which permit courts to set aside agency actions that are arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with the law. 5 U.S.C. § 706(2)(a). This claim relies on an attempt to improperly expand the scope of 28 C.F.R. Part 23. Contrary to Plaintiffs' assertions, that regulation does not establish the standard for all information-sharing overseen by the federal government. It is a regulation of limited applicability that places conditions on "criminal intelligence systems" receiving funding pursuant to a particular statutory source, the Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act), Pub. L. 90-351, 82 Stat. 197, codified at 42 U.S.C. § 3711 *et seq.* Plaintiffs' claims based on 28 C.F.R. Part 23 fail for several reasons.

First, Plaintiffs seek to facially invalidate the Functional Standard in its entirety (and not just with respect to the specific circumstances of the Plaintiffs) because it purportedly does not adhere to the standards in 28 C.F.R. Part 23, but they cannot meet the requirements needed to succeed on such a challenge. To prevail on a facial challenge, a plaintiff "must establish that no set of circumstances exists under which the regulation would be valid." *Reno v. Flores*, 507 U.S. 292, 301 (1993); *see also Akhtar v. Burzynski*, 384 F.3d 1193, 1198 (9th Cir. 2004). Plaintiffs cannot make any such showing for the simple reason that the Functional Standard has applications other than to "criminal intelligence systems" funded through support of the Omnibus Act. As is clear on the face of that document, the Functional Standard applies to the sharing of SARs in connection with the NSI regardless of whether the information-sharing system is funded through the Omnibus Act. There are

therefore at least some applications of the Functional Standard that plainly would not be in conflict with 28 C.F.R. Part 23.

Second, even if Plaintiffs had identified a particular application of the Functional Standard purportedly subject to 28 C.F.R. Part 23, their challenge effectively would seek to compel the agency responsible for implementing Part 23—the Office of Justice Programs (OJP)—to take an enforcement action with respect to a specific, non-compliant information-sharing system used in connection with the NSI. But whether the OJP should take a particular enforcement action is a decision committed to agency discretion and thus not subject to APA review. Moreover, even if Plaintiffs' could overcome this presumption against enforcement, no such enforcement would be appropriate in this instance. The only information-sharing system currently used in connection with the NSI is the NSI SAR Data Repository, which is operated by the Federal Bureau of Investigation (FBI). The FBI has not and does not receive any Omnibus Act funding for that information-sharing system, and thus, there would be no basis for the OJP to require the FBI to operate the NSI SAR Data Repository in accordance with the requirements of 28 C.F.R. Part 23.

Third, turning to the merits of the Functional Standard, there is ample evidence in the administrative record supporting the reasonableness of the PM-ISE's decision not to adopt the "reasonable suspicion" standard. Pursuant to its statutory authorization under the IRTPA, the PM-ISE was directed to adopt a framework for the sharing of SAR information that balanced the needs of national security against the privacy and civil liberty interests of individuals. Consistent with that authority, and based on collaboration with other law enforcement entities, the PM-ISE determined that the "reasonably indicative" operational concept best achieved that difficult objective. Plaintiffs claim that this decision was arbitrary and capricious because the PM-ISE should have adopted the "reasonable suspicion" standard in 28 C.F.R. Part 23. But there is nothing in the PM-ISE's statutory mandate that required adoption of the mandates of this regulation—which was issued by a different

federal agency, pursuant to a separate statutory authorization, and for a different purpose. Plaintiffs' disagreement with a reasonable policy determination fails to establish an APA violation.

BACKGROUND

I. Statutory and Regulatory Background

Following the September 11, 2001 attacks, it became apparent that law enforcement entities within the United States were not adequately sharing the intelligence information needed to conduct counterterrorism operations effectively. *See* Suppl. A.R. at 23.[1] To remedy this shortcoming, both the President and Congress took actions to establish an information sharing environment (ISE) that would improve the free flow of pertinent information between federal, state, local, tribal, and territorial governments, and where appropriate, private sector and foreign partners. The ISE is not a single database, or set of databases, used to share information. It is a "decentralized, distributed, and coordinated environment" that "provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies." 6 U.S.C. § 485(b)(2).

The President created the ISE in August 2004 through Executive Order 13556. Exec. Order No. 13356, 69 Fed. Reg. 53,599 (Aug. 27, 2004). Shortly thereafter, in December 2004, Congress passed Section 1016 of IRTPA to provide congressional support for the development of the ISE. Section 1016 directs the President to (1) "create an [ISE] for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties"; (2) "designate the

[1] Citations to the Administrative Record, ECF Nos. 53, 79–1, 79–2, are abbreviated "A.R." and citations to Supplemental Administrative Record, ECF No. 107, are abbreviated "Suppl. A.R." Citations to the A.R. include two documents that were inadvertently omitted from the initial Administrative Record, ECF No. 79-1, and corrected versions of six pages from the initial Administrative Record that were inadvertently reduced in size from the original or contained inadvertent redactions, ECF No. 79-2.

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).

The IRTPA also created the office of the Program Manager for the Information Sharing Environment (PM-ISE) to assist the President in performing these duties. 6 U.S.C. § 485(f). The PM-ISE, 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 PM-ISE is appointed by the President. *Id.* § 485(f)(1).

II. The Nationwide Suspicious Activity Reporting Initiative

As part of the effort to develop the ISE, the President issued guidance directing the PM-ISE to develop a framework for the sharing of SARs related to terrorism. In October 2007, the President released his National Strategy for Information Sharing, which outlines the responsibilities of federal, state, local, tribal, and territorial governments in improving terrorism-related information sharing. Suppl. A.R. at 11-58. That strategy, among other things, 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 54–55. The President further instructed that this framework should promote the broad sharing of information related to terrorism across jurisdictional lines while protecting the privacy and civil liberty of individuals to the greatest extent practicable. *See id.* at 2, 9, 21, 123, 165; Suppl. A.R. at 33.

In response, the federal government—in collaboration with federal, state, local, tribal, and territorial government entities—developed the NSI. Under long-standing

practice, law enforcement gathers tips and leads regarding behaviors and incidents associated with crime, records those tips and leads in SARs, and shares them (as appropriate) with other law enforcement entities. *Id.* at 162–74, 189–90. The NSI seeks to build on that practice by establishing "standardized processes and policies that provide the capability" for all level of governments to share SARs related to terrorism "through a distributed information sharing system that protects privacy, civil rights, and civil liberties." A.R. at 348. NSI participants include law enforcement, homeland security, and other information-sharing partners at the federal, state, local, tribal, and territorial government level. *Id.* at 422. The objective of the NSI is to provide specific indications about future acts of terrorism that might not be detectable in the absence of information sharing across jurisdictional lines, as well as to allow for the analysis of terrorism-related trends and patterns on a nationwide basis. *Id.* at 422, 428.

III. The Functional Standard for Suspicious Activity Reporting

Consistent with Presidential guidance, and to support the development of the NSI, the PM-ISE released the Functional Standard, version 1.0, in January 2008. A.R. at 75–106. The Functional Standard is a policy document that "allows for [the Nationwide SAR process] to occur in a standardized manner by documenting information exchanges and business requirements, and describing the structure, content, and products, associated with processing, integrating, and retrieving [SARs] by ISE participants." *Id.* at 190; *see also id.* 417 (explaining that the Functional Standard is "Guidance" that "describes the structure, content, and products associated with processing, integrating, and retrieving [terrorism-related SARs] by ISE agencies participating in the NSI."). The Functional Standard has been updated twice: version 1.5 was released in May 2009, *id.* at 192–227, and version 1.5.5 was released in February 2015, *id.* at 414–73.

The development of the Functional Standard was a collaborative process that allowed for significant participation by numerous groups—including NSI participants and

advocacy organizations. *See generally* Decl. of Basil N. Harris (Harris Decl.), attached as Exhibit A. Prior to the release of each update of the Functional Standard, the PM-ISE informed these interested parties that the Functional Standard was going to be updated, allowed them the opportunity to provide input regarding those updates, and provided an explanation of the recommendations that were adopted or rejected, as well as the reasons for those decisions. *See id.* Among other things, the PM-ISE held meetings with representatives of NSI participants at all levels of government, as well as with representatives of privacy and civil liberties organizations *See id.* ¶¶ 8–9, 13–14. The PM-ISE also received oral and written input from these interested parties in response to its request for comments. *See id.* ¶¶ 10, 15. This approach was consistent with the direction—provided by the President, the Director of National Intelligence, and Congress—that the development of the ISE should be collaborative. *See id.* ¶¶ 3–6.

Importantly, the Functional Standard is not intended to provide guidance for all information collection and sharing within the government. The Functional Standard only provides guidance for the sharing of SARs in connection with the NSI. A.R. at 429. Indeed, though the Functional Standard provides guidance for any NSI information-sharing system, there is currently only one information-sharing system used in connection with the NSI: the NSI SAR Data Repository. *Id.* at 415, 429.[2] The Functional Standard does not alter the legal standards that apply when law enforcement officers gather information, regardless of whether that information is ultimately shared through an NSI information-sharing system. *Id.* at 423–24. It also does not override any legal authorities permitting the sharing of information outside the context of an NSI information-sharing system, including the sharing of terrorism-related tips and leads with the FBI for investigative follow up. *Id.* at 429–30. In

[2] The NSI SAR Data Repository is housed within eGuardian—an unclassified, web-based system for receiving, tracking, and sharing SARs in the NSI, as well as receiving and documenting other terrorism-related information and other cyber or criminal threat information. A.R. at 416.

other words, the Functional Standard is intended only to describe the practices that should be followed before a SAR is made available to all other NSI participants through an NSI information-sharing system, such as the NSI SAR Data Repository.

As explained by the Functional Standard, a SAR undergoes a two-part review process by a trained analyst before it is made available to other NSI participants in an NSI information-sharing system. *Id.* at 427. First, it is reviewed against sixteen pre-operational behaviors associated with terrorism that are identified in the Functional Standard. *Id.* at 427, 454–64.[3] Second, if the information reflects one or more of those behaviors, the analyst determines whether—based on the available context, facts, and circumstances—the SAR has a potential nexus to terrorism. *Id.* at 427. If the SAR is determined to have such a nexus, it is submitted to an NSI information-sharing system, which makes that information available to other NSI participants. *Id.* at 427. Even after submission, however, the SAR remains under the ownership and control of the submitting organization and may be removed from the NSI information-sharing system by that organization. *Id.* at 428.

Relevant to this lawsuit, the Functional Standard includes guidance for analysts identifying the SARs that have a potential nexus to terrorism and thus should be broadly shared with NSI participants. Specifically, the Functional Standard instructs that SARs should only be shared through an NSI information-sharing system when an analyst determines (based on the two-step process described above) that the SAR contains "observed behavior" that is "reasonably indicative of pre-operational planning associated with terrorism or other criminal activity." A.R. at 417. As reflected in the most recent version of the Functional Standard, "reasonably indicative" is not a strict standard that must be rigidly applied by analysts. It is an "*operational concept* for documenting and sharing suspicious activity report[s]" that "creates in the mind of the reasonable observer, including a

---

[3] An example of a pre-operational behavior is compromising or disrupting (or attempting to compromise or disrupt) an organization's information technology structure. *Id.* at 457.

law enforcement officer, an articulable concern that the behavior may indicate pre-operational planning associated with terrorism or other criminal activity." *Id.* at 417 (emphasis added). The Functional Standard further emphasizes that this determination requires an analyst to apply his or her "professional judgment" to all the "available context, facts, and circumstances." *Id.* at 427.

IV. Criminal Intelligence Systems Funded by the Omnibus Act

The Omnibus Act is a separate and distinct statute from the IRTPA, which was not enacted until 2004. According to the Omnibus Act's preamble, Congress found it necessary to pass that statute to assist state and local governments in reducing the high incidence of crime, which Congress found to be "essentially a local problem." 82 Stat. 197. To achieve that goal, the Omnibus Act (among other things) created the OJP, a bureau of the Department of Justice that oversees federal grants for the implementation of crime fighting technologies and strategies by state and local governments. *See generally* 42 U.S.C § 3711, 3713–16.[4]

The OJP issued 28 C.F.R. Part 23 pursuant to its statutory authority to regulate federal grants provided under the Omnibus Act. More specifically, the Omnibus Act authorizes the OJP to issue policy standards governing the collection, maintenance, and dissemination of "criminal intelligence" in "criminal intelligence systems" that operate through support of the Omnibus Act. 42 U.S.C. § 3789g(c).[5] The Omnibus Act does not define the terms "criminal intelligence" or "criminal intelligence systems." The OJP, however, has defined a "criminal intelligence system" as "the arrangements, equipment,

---

[4] The OJP was previously known as the Law Enforcement Assistance Administration but was reconstituted as the OJP in 1984. Joint Resolution, Pub. L. 98-473, 98 Stat. 1837 (1984).

[5] In addition to its specific statutory authority to issue regulations for "criminal intelligence systems" receiving funding pursuant to the Omnibus Act, the 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).

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). It has further defined "criminal intelligence information" as "data which has been evaluated to determine that it . . . [i]s relevant to the identification of a criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity." *Id.* § 23.3(b)(3)(i). In short, the purpose of a criminal intelligence system is to collect information and intelligence about the identity and criminal activity of suspects who are being investigated for their involvement in a criminal enterprise. *See also* 28 C.F.R. § 23.2 (explaining that certain types of crimes require "some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area" and that "[t]he exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities").

Consistent with the OJP's statutory authority, the applicability of 28 C.F.R. Part 23, is expressly limited to "criminal intelligence systems" operating through support of the Omnibus Act. 28 C.F.R. §§ 23.1, 23.3(a). As a condition of funding, those "criminal intelligence systems" are required to comply with a variety of operating principles. *Id.* § 23.20. For purposes of this lawsuit, only one of those operating principles is relevant. That principle provides that a "project," defined in the regulation as the organizational unit operating a "criminal intelligence system," *id.* § 23.3(b)(5), "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." *Id.* § 23.20(a). The failure to comply with the requirement that "reasonable suspicion" be established before information is collected about an individual may result in the withholding of funding from the entity operating the "criminal intelligence system," *see* 28 C.F.R. §§ 23.30, 23.40, or the imposition of a fine up to $10,000 on that entity, *see* 42 U.S.C. §§ 3789g(d). The OJP has also established specific

mechanisms for monitoring whether projects receiving Omnibus Act funding are in compliance with the requirements of 28 C.F.R. Part 23. *See* 28 C.F.R. §§ 23.30, 23.40.

STANDARD OF REVIEW

The PM-ISE has filed an Administrative Record, ECF Nos. 53, 79–1, 79–2, and a Supplemental Administrative Record, ECF No. 107, in this matter. Consistent with the Magistrate Judge's and District Court's Orders, *see* ECF Nos. ECF Nos. 88, 102, the scope of the combined administrative record is limited to all documents and materials directly or indirectly considered by the agency in deciding to use the "reasonably indicative" operational concept in the Functional Standard instead of adopting the "reasonable suspicion" standard articulated in 28 C.F.R Part 23. *See* ECF No. 107-1.[6] Following the PM-ISE's filing of that administrative record, the parties have agreed that it is appropriate for this case to proceed to summary judgment. *See* ECF No. 110.

The standard of review in an APA case is different than the standard of review typically applied when a court resolves a motion for summary judgment. *See Klamath Siskiyou Wildlands Ctr. v. Gerritsma*, 962 F. Supp. 2d 1230, 1233 (D. Or. 2013), *aff'd sub nom. Klamath-Siskiyou Wildlands Ctr. v. Gerritsma*, 638 F. App'x 648 (9th Cir. 2016); *San Joaquin River Grp. Auth. v. Nat'l Marine Fisheries Serv.*, 819 F. Supp. 2d 1077, 1083–84 (E.D. Cal. 2011). Under Federal Rule of Civil Procedure 56(c), summary judgment is appropriate where "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to

---

[6] In addition to challenging the Functional Standard, Plaintiffs' Complaint asserts two identical claims challenging a purported "DOJ Standard" for information sharing that is distinct from the Functional Standard. *Compare* Am. Compl. ¶¶ 159–64, 167–59 (Functional Standard) *with id.* ¶¶ 153–58, 165–66 (DOJ Standard). As Defendants have explained, no such standard exists and thus Defendants have not submitted an administrative record for that purported standard. *See* ECF No. 56. This is consistent with the decision of this Court denying Plaintiffs' motion seeking to take discovery regarding the alleged existence of a separate DOJ standard. *See* ECF No. 60. Accordingly, because no such standard exists, Defendants request that the Court grant summary judgment on Plaintiffs' claims regarding the purported "DOJ Standard," which are no more than surplusage to Plaintiffs' claims regarding the Functional Standard.

judgment as a matter of law." In a case involving review of agency action under the APA, however, the district court's role is not to identify genuine disputes of material fact for trial because no trial is anticipated or would be appropriate in such a case. *Klamath Siskiyou Wildlands Ctr.*, 962 F. Supp. 2d at 1233; *see also Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 89 (D.D.C. 2006) ("[T]he standard set forth in Rule 56(c) does not apply [in an APA case] because of the limited role of a court in reviewing the administrative record."); *McCrary v. Gutierrez*, 495 F. Supp. 2d 1038, 1041 (N.D. Cal. 2007) (judicial review of agency action under the APA limited to the administrative record).

Instead, "[u]nder the APA, it is the role of the agency to resolve factual issues to arrive at a decision that is supported by the administrative record, whereas 'the function of the district court is to determine whether or not as a matter of law the evidence in the administrative record permitted the agency to make the decision it did.'" *Sierra Club*, 459 F. Supp. 2d at 90 (quoting *Occidental Eng'g Co. v. INS*, 753 F.2d 766, 769–70 (9th Cir.1985)). In other words, "the district court acts like an appellate court, and the 'entire case' is 'a question of law.'" *Nat'l Law Ctr. on Homelessness & Poverty v. U.S. Dep't of Veterans Affairs*, 842 F. Supp. 2d 127, 130 (D.D.C. 2012) (quoting *Amer. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1083 (D.C. Cir. 2001)). "Summary judgment thus serves as the mechanism for deciding, as a matter of law, whether the agency action is supported by the administrative record and otherwise consistent with the APA standard of review." *Stuttering Found. of Am. v. Springer*, 498 F. Supp. 2d 203, 207 (D.D.C. 2007).

ARGUMENT

I. Plaintiffs' Notice-and-Comment Claim Fails

Plaintiffs' notice-and-comment claim fails for two reasons. First, the PM-ISE was not required to go through notice-and-comment rulemaking when it issued the Functional Standard because that document was issued as policy guidance for NSI participants, and not pursuant to that agency's legislative function. Second, even if the PM-ISE was required to

observe the APA's rulemaking procedures when issuing the Functional Standard, any such error was harmless because the development of the Functional Standard was a collaborative process that allowed robust participation by interested parties.

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

The notice-and-comment procedures of the APA do not apply to every agency pronouncement. Agencies to which Congress has delegated legislative authority are empowered to issue rules that have the same power and effect as statutory enactments. *See Erringer v. Thompson*, 371 F.3d 625, 630 (9th Cir. 2004); *Prod. Tool Corp. v. Employment & Training Admin., U.S. Dep't of Labor*, 688 F.2d 1161, 1165 (7th Cir. 1982). When agencies issue legislative rules, they are required to follow the public rulemaking process articulated in the APA as a procedural check on that delegated authority. 5 U.S.C. § 553. But when an agency pronouncement does not reflect an exercise of the agency's legislative function, the APA's rulemaking procedures do not apply.

In particular, the APA explicitly exempts "general statements of policy" from its procedural requirements. 5 U.S.C. § 553(b)(3)(A). Unlike a legislative rule, a general statement of policy binds neither courts nor the agency. *See Brock v. Cathedral Bluffs Shale Oil Co.*, 796 F.2d 533, 536 (D.C. Cir. 1986). Instead, these policy statements serve the dual function of informing the public of how the agency intends to exercise its discretionary powers and providing direction to the agency's personnel regarding the exercise of that discretion. S*ee Mada-Luna v. Fitzpatrick*, 813 F.2d 1006, 1013 (9th Cir. 1987).

The Court of Appeals for the Ninth Circuit has addressed when an agency pronouncement is a general statement of policy rather than a legislative rule. As explained by that Court, in determining whether an agency rule is a general statement of policy, courts are not to look to the substantive impact of the pronouncement on the public at large but to the effect of the pronouncement on agency decision-making. *Mada-Luna*, 813 F.2d at 1016; *see also Colwell v. Dep't of Health & Human Servs.*, 558 F.3d 1112, 1124 (9th Cir. 2009); *see also*

Brock, 796 F.2d at 537. The Court further instructed courts to look to the "language and structure" of an agency pronouncement in determining whether it is a legislative rule or a general statement of policy. *Mada-Luna*, 813 F.2d at 1015.

Applying this framework, it is clear that the Functional Standard, which is replete with language indicating that it constitutes policy guidance, is not a legislative rule. Among other things, the Functional Standard states that:

- The Functional Standard is "limited to *describing* the ISE-SAR process and associated information exchanges," A.R. at 414 (emphasis added);
- The Functional Standard is intended to promote the "*standardized and consistent* sharing" of SARs, *id.* at 422 (emphasis added);
- The "ISE-SAR process offers a *standardized means* for identifying and sharing ISE-SARs and applying data analytic tools to the information," *id.* at 424 (emphasis added);
- "The NSI establishes *standardized processes and policies*," *id.* at 416 (emphasis added); and
- The Functional Standard "*describes the structure, content and products* associated with processing, integrating, and retrieving IS-SARs by ISE agencies participating in the NSI," *id.* at 417 (emphasis added).

According to its own terms, therefore, the Functional Standard is descriptive in nature: It describes a standardized process (developed through a collaborative effort among NSI participants) for sharing SARs. Consistent with that descriptive purpose, the Functional Standard does not use any imperative terms (*e.g.*, "shall") when describing the process for sharing SARs within the NSI. Indeed, the Functional Standard explicitly provides that it may be "customized" for "unique communities." *Id.* at 429.

The treatment of the "reasonably indicative" operational concept in the Functional Standard further emphasizes that this agency pronouncement is a statement of policy rather than a binding legislative rule. The first version of the Functional Standard stated that NSI participants may share SARs after determining that they are potentially related to terrorism.

A.R. at 80. In response to concerns raised by advocacy groups, the subsequent versions of the Functional Standard have explained that a SAR has a potential nexus to terrorism when it is "reasonably indicative of pre-operational planning associated with terrorism." *Id.* at 193, 200, 427. Rather than describing the term "reasonably indicative" as a binding standard or rule, however, the Functional Standard describes it as an "operational concept," *id.* at 417, that requires the application "professional judgment" in light of the "available context, facts, and circumstances," *id.* at 427. *See also id.* at 428 (stating that the vetting of SAR is an "analytical process . . . subject to further review and validation," and that SARs submitted to an information-sharing system used in connection with the NSI remain under the "ownership and control" of the submitting organization).[7] In sum, the "reasonably indicative" operational concept acts as a guidepost for NSI participants within the Functional Standard's framework. It is not a strict legal standard or rule with which NSI participants must comply or else face sanction.

Indeed, the Functional Standard does not even contemplate the possibility of sanctions being imposed on NSI participants. The regulation on which Plaintiffs' base their substantive claims in this case, 28 C.F.R. Part 23, provides a useful contrast in this regard. Unlike the Functional Standard, 28 C.F.R. Part 23 explicitly states that the "criminal intelligence systems" subject to its requirements "shall" comply with certain operating principles. 28 C.F.R. § 23.20. And consistent with the mandatory nature of that regulation, the OJP and Congress have both established specific mechanisms for monitoring whether

---

[7] Prior to determining whether a SAR is reasonably indicative of pre-operational planning associated with terrorism, the Functional Standard also instructs analysts to compare the behavior reported in the SAR against to a list of sixteen pre-operational behaviors that may be associated with terrorism. A.R. at 427. The Functional Standard describes this list of behaviors as "criteria guidance," states that the application of these criteria requires the analyst to take into account "the context, facts, and circumstances" of the observed behavior, and emphasizes "the importance of having a trained analyst or investigator" conduct this analysis. *Id.* at 454–64.

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

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

* * *

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

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

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

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

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

not prejudice the petitioner, it would be senseless to vacate and remand for reconsideration." *PDK Labs. Inc. v. D.E.A.*, 362 F.3d 786, 799 (D.C. Cir. 2004).

The Court of Appeals for the Ninth Circuit has addressed when an agency's failure to observe the APA's procedural requirements is harmless. Specifically, that Court has stated that a failure to provide adequate notice and comment is harmless where the agency's error "clearly had no bearing on the procedure used or the substance of decision reached." *Riverbend Farms, Inc. v. Madigan*, 958 F.2d 1479, 1487 (9th Cir. 1992). This standard requires the court to look at the error's effect on the procedural process and substantive outcome, but it does not mean that any shortcoming in the procedural process is per se harmful; indeed, such a standard would mean that no procedural error could ever be harmless. Instead, this standard requires district courts to consider whether the procedural errors meaningfully impacted the agency's decision-making process. In *Safari Aviation, Inc., v. Garvey*, 300 F.3d 1144 (9th Cir. 2002), for example, the Court of Appeals determined that an agency's failure to examine the petitioner's comments before promulgating a final rule was harmless because the substance of those comments had already been considered by the agency in previous rulemaking proceedings. *Id.* at 1152.

The Supreme Court's decision in *Shinseki v. Sanders*, 556 U.S. 396 (2009), confirms that harmless error analysis must focus on whether a procedural error has caused actual prejudice.[8] In that decision, the Court explained that, in addition to assessing whether a procedural error is likely to have had a substantive impact on an agency's ultimate decision, a reviewing court applying the harmless error rule might also consider the error's "likely effects on the perceived fairness, integrity, or public reputation of [agency] proceedings." *Id.* at 411–12. The Court also made clear that a court's harmless error review cannot rely on

---

[8] Though *Sanders* addressed the harmless error standard in the context of appeals from the United States Court of Appeals for Veterans Claims, the Supreme Court made clear that its analysis of the harmful error rule applies to judicial review under the APA. *Id.* at 406–07.

mandatory presumptions of prejudice whenever a procedural error is identified. *Id.* at 407–08. The Court further held that the burden of showing that an error is harmful falls upon the party attacking the agency's determination. *Id.* at 409–10.[9]

Applying this standard, the PM-ISE's failure to observe the APA's technical requirements cannot be considered harmful. Consistent with guidance provided by the President and the Director of National Intelligence, as well as the IRTPA, the development of the Functional Standard was a collaborative process that allowed for significant participation by interested parties—including NSI participants and advocacy organizations representing the privacy and civil liberty interests of individuals. *See* Harris Decl. ¶¶ 3–6. Prior to the release of each update of the Functional Standard, the PM-ISE informed these interested parties that the Functional Standard was going to be updated, allowed them the opportunity to provide input regarding those updates, and provided an explanation of the recommendations that were adopted or rejected, as well as the reasons for those decisions. *See id.* ¶¶ 7–17. This process is consistent with the general structure of the APA's notice-and-comment procedures—which require the agency to provide notification of the proposed rule to interested parties, allow those parties the opportunity to comment, and provide a concise statement of its reasons. 5 U.S.C. §§ 553 (b)–(c).

Indeed, the only substantive dispute in this matter—the PM-ISE's adoption of the "reasonably indicative" operational concept rather than the "reasonable suspicion" standard used in 28 C.F.R. Part 23—was an outgrowth of discussions between the PM-ISE and advocacy groups during the development of the Functional Standard. In response to the

---

[9] The Ninth Circuit Court of Appeals has stated that its harmless error formulation—that a harmless error is one that "had no bearing on the procedure used or the substance of decision reached"—survives the Supreme Court's decision in *Sanders*. *See Cal. Wilderness Coal. v. U.S. Dep't of Energy*, 631 F.3d 1072, 1092 (9th Cir. 2011). But that standard must still be interpreted in a manner that is consistent with the Supreme Court's instruction that harmless error analysis cannot rely on any presumption that a procedural error is per se harmful.

PM-ISE's request for comments on potential amendments to Functional Standard 1.0, a representative of the American Civil Liberties Union (ACLU) suggested amending the definition of suspicious activity to "behavior *reasonably indicative* of pre-operational planning related to terrorism or other criminal activity." A.R. at 158 (emphasis added). The PM-ISE adopted that proposed definition when it issued Functional Standard 1.5, as well as several other changes suggested by the ACLU. *Id.* at 193. The ACLU and other civil liberties groups subsequently proposed, during discussions regarding potential amendments to Functional Standard 1.5, that the "reasonably indicative" operational concept be replaced with the "reasonable suspicion" standard articulated in 28 C.F.R. Part 23. *Id.* at 330–34. The PM-ISE, as noted, declined to include that amendment in Functional Standard 1.5.5 and provided an official explanation for that decision. *Id.* at 345. But that ultimate decision does not change the fact that interested parties, including advocacy groups representing Plaintiffs' interests, had ample notice of and the opportunity to participate in the development of the Functional Standard, did in fact participate in the Functional Standard's development, and, indeed, had some of their recommendations accepted.

In light of this collaborative process, Plaintiffs cannot establish that the purported procedural errors in this case resulted in any prejudice. The substantive outcome would have been the same because the PM-ISE had already considered and rejected the position that the Functional Standard should adopt the "reasonable suspicion" standard. And the procedure used would not have been meaningfully different because the PM-ISE provided notice that it intended to update the Functional Standard to interested parties, allowed them to provide comments regarding that potential update, and responded to those comments. In *Safari Aviation*, as noted, the Court of Appeals determined that the agency's procedural errors were harmless because that agency had already considered the content of the public comments that the petitioner asserted were relevant. *Safari Aviation*, 300 F.3d at 1152. For the same reason, because the PM-ISE has already considered and responded to the

substance of the very comments that Plaintiffs assert they were entitled to make, remand is not warranted in this case.

II. Plaintiffs' Arbitrary-and-Capricious Claim Fails

Plaintiffs' arbitrary-and-capricious claim relies on an attempt to improperly expand the scope of 28 C.F.R. Part 23. Contrary to Plaintiffs' assertions, that regulation does not establish the standard for all information-sharing overseen by the federal government. It is a regulation of limited applicability that places funding conditions on "criminal intelligence systems" receiving funding from a particular statutory source, the Omnibus Act. The limited scope of 28 C.F.R. Part 23 undermines Plaintiffs' claims in several respects. First, Plaintiffs' arbitrary-and-capricious claim is structurally deficient because it seeks to facially invalidate the Functional Standard even though it is clear on the face of that document that the Functional Standard has applications other than "criminal intelligence systems" funded through support of the Omnibus Act. Second, the decision whether to enforce 28 C.F.R. Part 23 against an organization operating a "criminal intelligence system," as that term is defined by Part 23, is committed to the discretion of the agency (the OJP) responsible for enforcing that funding regulation. Indeed, the only information-sharing system currently used in connection with the NSI (the NSI SAR Data Repository) is in fact not funded through the Omnibus Act, making any such enforcement unwarranted. Third, the administrative record establishes that the Functional Standard and 28 C.F.R. Part 23 concern different aspects of the law enforcement process, and thus, it was entirely reasonable for the PM-ISE to adopt the "reasonably indicative" operational concept rather than the "reasonable suspicion" standard articulated in Part 23.

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

Plaintiffs bring a facial challenge to the "reasonably indicative" operational concept, asserting that is in conflict with the "reasonable suspicion" standard articulated in 28 C.F.R. Part 23. The difference between a facial and as-applied challenge can be discerned in part by

looking at the requested remedy. Where a "claim and the relief that would follow . . . reach beyond the particular circumstances of [the parties asserting the challenge]," the challenge is facial in nature and it must "satisfy [the applicable legal] standards for a facial challenge to the extent of that reach." *John Doe No. 1 v. Reed*, 561 U.S. 186, 194, (2010); *see also Family PAC v. McKenna*, 685 F.3d 800, 808 n.5 (9th Cir. 2012); *Ctr. for Individual Freedom v. Madigan*, 697 F.3d 464, 475 (7th Cir. 2012). Here, Plaintiffs seek to invalidate the "reasonably indicative" operational concept in its entirety and not just with respect to the particular circumstances of the Plaintiffs. They must accordingly meet the applicable standards for a facial challenge, which they cannot do.

The requirements for a facial challenge are significantly more demanding than the requirements that must be satisfied to bring an as-applied challenge. To prevail on a facial challenge, a plaintiff "must establish that no set of circumstances exists under which the regulation would be valid." *Reno v. Flores*, 507 U.S. 292, 301 (1993); *see also Akhtar v. Burzynski*, 384 F.3d 1193, 1198 (9th Cir. 2004). In other words, it is not enough to establish a hypothetical case or hypothetical cases where a regulation might lead to an outcome that is arbitrary, capricious, an abuse of discretion, or otherwise contrary to law. *Ass'n of Private Sector Colleges & Universities v. Duncan*, 110 F. Supp. 3d 176, 195–96 (D.D.C. 2015). The plaintiff must show that the regulation would be invalid regardless of its application to any particular hypothetical case. This requirement for facial challenges applies regardless of whether the source of the challenge is constitutional, statutory, or (as here) regulatory. *Reno*, 507 U.S. at 301.

Plaintiffs cannot satisfy this unequivocal requirement because 28 C.F.R. Part 23 only applies to "criminal intelligence systems" receiving Omnibus Act funding, whereas the Functional Standard recommends the use of the "reasonably indicative" operational concept for all information-sharing systems used in connection with the NSI regardless of their funding source. This means that, at a minimum, any application of the "reasonably

indicative" operational concept to an information-sharing system not funded through support of the Omnibus Act would not conflict with 28 C.F.R. Part 23.

As noted, 28 C.F.R. Part 23 is a limited regulation that imposes conditions on criminal intelligence systems operating through funding support under the Omnibus Act. *See* 28 C.F.R. §§ 23.1, 23.3. Contrary to Plaintiffs' suggestion, therefore, Part 23 does not establish a general prohibition on the collection, maintenance, and sharing of information in the absence of reasonable suspicion but only places restrictions on "criminal intelligence systems" receiving funding from a particular statutory source. Indeed, the OJP is not statutorily authorized to issue broad regulations governing all information sharing between federal, state, and local law enforcement authorities. It is only authorized to issue regulations governing "criminal intelligence systems" funded pursuant to the the Omnibus Act. *See* 42 U.S.C. § 3789g(c). Consistent with that statutory authority, the applicability of 28 C.F.R. Part 23 is expressly limited to "criminal intelligence systems operating through support under the Omnibus [Act]." 28 C.F.R. § 23.3(a).

The Functional Standard, in contrast, provides guidance to NSI participants sharing SAR information in connection with the NSI through any information-sharing system regardless of that system's funding source. A.R. at 414, 429–30. It is not limited to, or even intended for, projects operating criminal intelligence systems funded through the Omnibus Act. The Functional Standard does not reference the Omnibus Act, and its only reference to 28 C.F.R. Part 23 indicates that the information-sharing systems within the NSI are distinct from Part 23 criminal intelligence systems. *See id.* at 468 ("If [ISE-SAR information meets the reasonable suspicion standard for criminal intelligence information], the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 C.F.R. Part 23." (emphasis in original)). This is not surprising because neither the NSI nor the Functional Standard is an outgrowth of the Omnibus Act. They are part of the development of the ISE pursuant to the IRTPA—an entirely separate statutory scheme

intended to promote the sharing of terrorism information among all appropriate federal, state, local, tribal, and territorial government entities, and, where appropriate, with their private partners. *See generally* 6 U.S.C. § 485.

These distinctions between the Functional Standard and 28 C.F.R. Part 23 preclude Plaintiffs' facial challenge. To successfully bring a facial challenge, Plaintiffs (as noted) would have to show that no set of circumstances exist under which the Functional Standard's "reasonably indicative" operational concept would be valid. They plainly cannot do that because 28 C.F.R. Part 23 only applies to criminal intelligence systems funded through the Omnibus Act, and the Functional Standard may be applied to information-sharing conducted in connection with an NSI information-sharing system regardless of whether that system receives Omnibus Act funding. Plaintiffs, in short, are attempting to use a regulation that imposes funding conditions on a specific type of information-sharing system receiving support from a particular statutory source to impose those conditions on information-sharing systems developed pursuant to a separate statutory scheme. Because an NSI information-sharing system can exist apart from Omnibus Act funding, Plaintiffs are not able to satisfy the requirements necessary to succeed on that sort of broad, facial challenge.

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

Plaintiffs have also failed to raise—and cannot support—an as-applied challenge to the Functional Standard's "reasonably indicative" operational concept. At a minimum, an as-applied challenge would require Plaintiffs to demonstrate that: (i) a specific NSI information-sharing system using the "reasonably indicative" operational concept is subject to 28 C.F.R. Part 23 (*i.e.*, a "criminal intelligence system" operating through Omnibus Act funding) and (ii) it was arbitrary and capricious for the federal government not to require the organization operating that information-sharing system to comply with the requirements of

28 C.F.R. Part 23. Such a challenge is not reviewable under the APA and, even if it were subject to review, would fail in the face of the factual record.

First, the federal agency responsible for ensuring compliance with 28 C.F.R. Part 23 is the OJP, and Plaintiffs cannot compel the OJP, through an APA claim, to take an enforcement action against the operator of an NSI information-sharing system. The APA permits an aggrieved party to bring suit challenging an agency's decision not to take a discrete action, but there are strict limits on the reviewability of agency inaction. Among other things, there is a strict presumption that the decision not to take an enforcement action is committed to agency discretion and therefore unreviewable. *See Heckler v. Chaney*, 470 U.S. 821, 832 (1985); *City & Cty. of San Francisco v. U.S. Dep't of Transp.*, 796 F.3d 993, 1001–04 (9th Cir. 2015); 5 U.S.C. § 701(a)(2). Plaintiffs have not attempted to overcome that presumption, and would not be able to do so.

Instead, Plaintiffs appear to assume that they may directly enforce the operating principles of 28 C.F.R Part 23. Congress, however, did not create a private right of action to enforce that regulation.[10] Instead, Congress authorized the OJP to take specific enforcement actions against any entity operating a "criminal intelligence system" funded through support of the Omnibus Act that failed to comply with the requirements of 28 C.F.R. Part 23—including by withholding funding from the entity operating the criminal intelligence system,

---

[10] There is no private right of action to enforce 28 C.F.R. Part 23 because Congress has not created such a right. "Like substantive federal law itself, private rights of action to enforce federal law must be created by Congress. The judicial task is to interpret the statute Congress has passed to determine whether it displays an intent to create not just a private right but also a private remedy." *Alexander v. Sandoval*, 532 U.S. 275, 286-87 (2001). Moreover, although a federal agency can invoke a private right of action established by Congress in a regulation, it may not create that private right of action through the issuance of a regulation. *Id.* at 291. Applying these standards, there is no basis to infer that Congress intended to permit private enforcement of 28 C.F.R. Part 23 when it authorized OJP to issue regulations imposing particular conditions on criminal intelligence systems funded through support of the Omnibus Act. *See* 42 U.S.C. §§ 3782(a), 3789g(c).

see 28 C.F.R. §§ 23.30, 23.40, or imposing a fine up to $10,000 on that entity, *see* 42 U.S.C. § 3789g(d). And the APA itself does not supply a separate cause of action to permit judicial review of an agency's decision whether or not to take those sorts of enforcement actions because any such decision is an inherently discretionary act.[11] In short, Congress left it to the OJP to decide whether the standards in 28 C.F.R. Part 23, which Plaintiffs ask this Court to impose, are being properly applied and to sanction any violation.

Second, even if Plaintiffs were able to overcome the presumption against reviewability of enforcement decisions, their as-applied APA challenge would fail because the administrative record does not support a finding that an information-sharing system used in connection with the NSI is subject to 28 C.F.R. Part 23. As Functional Standard 1.5.5 clarifies, the only NSI information-sharing system that is currently in operation is the NSI SAR Data Repository, which is operated by the FBI within its eGuardian system. A.R. at 415. The FBI, however, does not receive any Omnibus Act funding for eGuardian or the NSI SAR Data Repository. The administrative record is devoid of any suggestion that the FBI receives such funding. And Defendants have further submitted a declaration from the OJP, which is exclusively responsible for providing federal grants under the Omnibus Act, establishing that the FBI has not and does not receive Omnibus Act funding for eGuardian or the NSI SAR Data Repository. *See* Decl. of Maryilynn B. Atsatt, attached as Exhibit B. Accordingly, any attempt to require enforcement of 28 C.F.R. Part 23 against the FBI based on its operation of eGuaridan would be meritless.

---

[11] For example, to determine whether to enforce 28 C.F.R. Part 23 against the operator of an information-sharing system, the OJP must determine whether the information-sharing system is a "criminal intelligence system" as that term is defined by Part 23, whether the information-sharing system operates through support of the Omnibus Act, and whether enforcement would serve the underlying purposes of the relevant statutory and regulatory framework.

C. The Challenged Decision Was Not Arbitrary or Capricious

Aside from the significant threshold problems with Plaintiffs' claim—*i.e.*, that the OJP has discretion to apply 28 C.F.R. Part 23 and that the only NSI information-sharing system currently in operation is not supported by the funding source that is the basis for that regulation—there is also ample support in the administrative record for the PM-ISE's decision to use the "reasonably indicative" operational concept rather than the "reasonable suspicion" standard. The PM-ISE, based in part on a recommendation by an advocacy organization, adopted the "reasonably indicative" operational concept in Functional Standard 1.5 because it determined that this operational concept reflected the appropriate balance between the competing interests of national security, on the one hand, and privacy and civil liberties, on the other hand. The PM-ISE later rejected the recommendation (again by certain advocacy organizations) that it replace the "reasonably indicative" operational concept with the "reasonable suspicion" standard in Functional Standard 1.5.5 because the PM-ISE determined that use of this standard was not feasible in light of the objectives of the NSI. Neither of those decisions was unlawful under APA standards.

1. *The APA's Arbitrary-and-Capricious Standard*

Judicial review under the APA's arbitrary-and-capricious standard is deferential and narrow. Section 706(2)(A) requires a reviewing court to uphold agency action unless it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). Under this standard, "[i]t is not the reviewing court's task to make its own judgment about the appropriate outcome. Congress has delegated that responsibility to the agency. The court's responsibility is narrower: to determine whether the agency complied with the procedural requirements of the APA." *San Luis & Delta-Mendota Water Auth. v. Locke*, 776 F.3d 971, 994 (9th Cir. 2014).

Accordingly, as the Supreme Court has explained, an agency rule (or in this case, functional standard) may only be deemed unlawful under the APA, if the agency has:

> [1] relied on factors which Congress has not intended it to consider, [2] entirely failed to consider an important aspect of the problem, [3] offered an explanation for its decision that runs counter to the evidence before the agency, or [4] is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.

Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983).

Plaintiffs' allegations asserting that the use of the "reasonably indicative" operational concept implicates constitutional concerns under the First Amendment, *see, e.g.*, Am. Compl., ECF No. 70, ¶¶ 1, 3–4, 29, 38, does not alter this standard of review. *See F.C.C. v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009). If Plaintiffs' contention is that the Functional Standard is unconstitutional, they could have asserted that claim. But Plaintiffs did not do so, and they may not alter the deferential arbitrary-and-capricious standard by suggesting that the agency action being reviewed may implicate constitutional concerns.

2. *The Adoption of the "Reasonably Indicative" Operational Concept*

Applying the deferential APA standard, there is ample evidence in the administrative record supporting the reasonableness of the PM-ISE's determination to adopt the "reasonably indicative" operational concept. Pursuant to its statutory authorization, the PM-ISE was directed to develop a framework for the sharing of SAR information among federal, state, local, tribal, and territorial entities that balanced the need of law enforcement to have access to pertinent SARs and the privacy and civil liberty interests of individuals. The PM-ISE considered these competing factors, as well as the input from NSI stakeholders and advocacy organizations, and selected the "reasonably indicative" operational concept. That decision-making process met the minimal standards of rationality imposed by the APA and should not be disturbed by this Court.

Following the release of Functional Standard 1.5, which was the first version of the Functional Standard to use the "reasonably indicative" operational concept, the PM-ISE provided a concise explanation of the reasons for its decision to provide that guidance:

> The use of the "reasonably indicative" determination process allows supervisors at source agencies and trained analysts and investigators at fusion

> centers and other agencies to have a uniform process that will result in better quality SARs and the posting of more reliable ISE-SARs to the ISE Shared Spaces, while at the same time enhancing privacy, civil rights, and civil liberties protections. Furthermore, this revision improves mission effectiveness and enables NSI participating agency personnel to identify and address, in a more efficient manner, potential criminal and terrorism threats by using more narrowly targeted language. Finally, better quality SARS should result in a sufficiently high quality of information enabling agencies and analysts to "connect the dots" while not producing so much information as to overwhelm agency analytical capacity.
>
> In addition, the "reasonably indicative" determination is an essential privacy, civil rights, and civil liberties protection because it emphasizes a behavior-focused approach to identifying suspicious activity and mitigates the risk of profiling based upon race, ethnicity, national origin, or religious affiliation or activity.

A.R. at 281–82. The PM-ISE, in other words, adopted the "reasonably indicative" operational concept based on a determination that it would promote the sharing of useful SAR information across jurisdictional lines while protecting privacy and civil liberties to the greatest extent practicable.

That decision was consistent with the PM-ISE's statutory mandate. Congress, as noted, directed the PM-ISE to issue "procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE" that were consistent with guidance provided by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget. 6 U.S.C. § 485(f)(2)(A)(iii). None of these entities instructed the PM-ISE to adopt any particular standard for the sharing of SAR information among federal, state, local, tribal, and territorial entities. Instead, they presented the PM-ISE with the difficult task of developing a framework for the sharing of SARs that balanced two competing factors: (1) the law enforcement need to have access to SAR information and (2) the protection of privacy interests and civil liberties. *See* A.R. at 2, 9, 21, 123, 165; Suppl. A.R. at 33–33.

The PM-ISE's decision reflects a careful balancing of those factors. Consistent with the collaborative approach to the NSI, the PM-ISE solicited input from NSI participants and

advocacy organizations based on their experience with the NSI following the release of Functional Standard 1.0. Based on the input received from those entities, the PM-ISE selected the "reasonably indicative" operational concept because it determined that this operational concept would allow for the effective sharing of SARs while protecting privacy and civil liberties. Indeed, as noted, it was an advocacy organization that recommended inclusion of the "reasonably indicative" operational concept. There is no basis for Plaintiffs' assertion that this decision reflects a failure to consider the factors mandated by statute or is otherwise unlawful.

3. *The Rejection of the "Reasonable Suspicion" Standard*

The PM-ISE also acted in a manner consistent with its statutory mandate in considering and rejecting a proposal by certain advocacy organizations to replace the "reasonably indicative" operational concept in the Functional Standard with the "reasonable suspicion" standard in 28 C.F.R. Part 23. *See* A.R. at 330-34, 345. The Functional Standard and 28 C.F.R. Part 23 were issued by two separate federal agencies (the PM-ISE and the OJP), pursuant to two separate statutory schemes (the IRTPA and the Omnibus Act), to support two different law enforcement processes (the sharing of tips and leads and the collection of criminal intelligence). Neither the APA nor any other federal law requires these agencies to adopt the same standards for separate and distinct law enforcement mechanisms.

The distinction between tips and leads (for SARs) and criminal intelligence is well developed in law enforcement. *See* A.R. at 162–74. Criminal intelligence is the product of an investigation that seeks to identify specific individuals and organizations engaged in criminal activity and to gather information about the criminal conduct in which they are engaged. *See id.* at 164 (defining "Criminal Intelligence Data" as "[i]nformation deemed relevant to the identification of and criminal activity engaged in by an individual or organization reasonably suspected of involvement in criminal activity."). SARs, in contrast, are reports of the initial tips and leads that law enforcement receive from a variety of sources

about suspicious activities. *See id.* at 164 (defining "Tips and Leads Data" as an "[u]ncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of criminal activity"); *id.* at 168 (explaining that "SARs" are "tips and leads"). Once collated and analyzed with correlating pieces of data from other sources, this SAR information may lead law enforcement to initiate a criminal investigation seeking to gather information about specific individuals and organizations suspected of being engaged in criminal conduct. *See id.* at 165–66. But this is a distinct law enforcement process that occurs outside the scope of the NSI and is not subject to the Functional Standard.

Based on these differences, the PM-ISE declined to follow the recommendation of certain advocacy organizations that the "reasonably indicative" operational concept in the Functional Standard be replaced with the "reasonable suspicion" standard articulated in 28 C.F.R. Part 23. *See* A.R. at 345. The PM-ISE, as noted, was directed to develop a framework for the NSI that promoted the broad sharing of SARs across jurisdictional lines while protecting privacy interests and civil liberties to the greatest extent practicable. Because the sharing of SARs occurs prior to the commencement of an investigation, the PM-ISE determined that it would not be feasible to continue to promote the broad sharing of SARs while requiring the establishment of reasonable suspicion before a SAR is shared. *See id.* That decision was based on the factors that the PM-ISE was required to consider by law and was within the bounds of reasonableness. Indeed, though the advocacy organizations' recommendation that the Functional Standard use the "reasonable suspicion" standard was discussed with NSI participants, no participant endorsed the adoption of that standard. *See id.*

In sum, the Functional Standard and 28 C.F.R. Part 23 have different purposes. The express purpose of 28 C.F.R. Part 23 is to impose operating principles on "Criminal Intelligence Systems" funded through support of the Omnibus Act that collect information

about individuals and organizations suspected of engaging in criminal conduct. 28 C.F.R. §§ 23.1, 23.2. The express purpose of the Functional Standard, in contrast, is to develop a framework for the sharing of SARs that allows law enforcement partners to "connect the dots" between suspicious activities occurring in different jurisdictions and, if appropriate, to take precautionary measures to prevent future acts of terrorism. A.R. at 422, 427–28. It was entirely reasonable for the OJP and the PM-ISE to take different approaches to these distinct programs.

III. Remand Without Vacatur Would Be the Only Appropriate Remedy

Assuming, *arguendo*, the Court contemplates granting some relief to Plaintiffs, their requested remedy would be improper as a matter of law. Plaintiffs ask this Court to enter a permanent injunction vacating the Functional Standard and requiring the PM-ISE "to use 28 C.F.R. Part 23 as the standard for SAR reporting." Am. Compl. at 37, Prayer for Relief ¶ 3. But the sole available remedy, again assuming any is warranted, would be a remand to the agency so that the PM-ISE can determine whether to re-issue the Functional Standard, and if so, the appropriate content of that Functional Standard. In no event can *this Court* order the issuance of a particular information-sharing standard, including by requiring adoption of 28 C.F.R. Part 23 for the NSI. That is not an available remedy upon judicial review under the APA.

Rather, there are only two available remedies when a court determines that an agency failed to satisfy the procedural requirements of the APA: remand *with* vacatur or remand *without* vacatur. *Cal. Comties. Against Toxics v. U.S. E.P.A.*, 688 F.3d 989, 992 (9th Cir. 2012); *see also* 5 U.S.C. § 706(2) (permitting a court to set aside agency action found to be unlawful). Whether an agency action should be vacated depends on the seriousness of the agency's errors and the disruptive consequence of an interim change. *See Cal. Comties.*, 688 F.3d at 992; *Pollinator Stewardship Council v. U.S. E.P.A.*, 806 F.3d 520, 532 (9th Cir. 2015). Courts

may also look to whether the agency is likely to adopt the same rule, or a similar rule, on remand. *Pollinator*, 806 F.3d at 532.

Applying this framework, if the Court determines that a remand is necessary, the Functional Standard should not be vacated during the remand period because doing so would result in an unacceptable risk of harm to national security. If the Functional Standard were vacated, the federal government would be left with two options: (1) operate the NSI without any information-sharing guidance; or (2) cease to operate the NSI. Both approaches would pose a significant risk to national security—resulting in either the oversharing or under-sharing of SAR information.[12] The Court of Appeals for the Ninth Circuit, in other cases, has held that the equities did not warrant vacating an agency decision where such a remedy would endanger a snail species, *Idaho Farm Bureau Fed'n v. Babbitt*, 58 F.3d 1392, 1405–06 (9th Cir. 1995), or pose a risk to the power supply, *Cal. Cmties.*, 688 F.3d at 994. If preventing these potential harms warrants judicial restraint, so does preventing the potentially significant harm to national security that would attend failing to share SARs with law enforcement agencies.

In the event of remand, moreover, it is likely that the PM-ISE would issue the same, or a substantially similar, Functional Standard. As explained, the PM-ISE already considered and rejected the proposal that the Functional Standard adopt the "reasonable suspicion" standard articulated in 28 C.F.R. Part 23. Accordingly, even if the agency were required to follow the notice-and-comment procedures contained in the APA, it is likely that the "reasonably indicative" operational concept would continue to be used in connection with the NSI.

As discussed above, the Court should uphold the Functional Standard, which was issued in accordance with the APA's requirements. But in any event, the Functional

---

[12] Operating the NSI without any information-sharing guidance might also result in increased risk to the privacy and civil liberty interests of individuals.

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

CONCLUSION

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

August 18, 2016

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ *Kieran G. Gostin*
Kieran G. Gostin
Trial Attorney
Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
Telephone: (202) 353-4556
Facsimile: (202) 616-8460
E-mail: kieran.g.gostin@usdoj.gov

Attorneys for Federal Defendants

CERTIFICATE OF SERVICE

I hereby certify that on August 18, 2016, I filed the above document and its attachments with the Court's CM/ECF system, which will send notice of such filing to all parties.

Date: August 18, 2016

/s/ *Kieran G. Gostin*
Kieran G. Gostin

EXHIBIT A

BENJAMIN C. MIZER
Principal Deputy Attorney General
ANTHONY J. COPPOLINO
Deputy Branch Director
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) 353-4556
Facsimile: (202) 616-8460
E-mail: kieran.g.gostin@usdoj.gov

Attorneys for Federal 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) (KAW)

DECLARATION OF BASIL N. HARRIS

I, Basil N. Harris, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am the Chief of Staff to the Office of the Program Manager for the Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence (ODNI), and have held that position since January 2, 2006. I am executing this declaration in support of the Government's motion for summary judgment in this case. The statements made herein are based on my personal knowledge, on my review of relevant information contained within the Administrative Record, and on information I obtained in the course of my official duties.

2. PM-ISE is responsible for the development of the Functional Standard for Suspicious Activity Reporting (Functional Standard) associated with the Nationwide Suspicious Activity Reporting Initiative (NSI). The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), among other things, made PM-ISE responsible for issuing procedures, guidelines, instructions, and functional standards that are consistent with the direction and policies issued by the President, the Director of the National Intelligence (DNI), and the Director of the Office of Management and Budget. The Functional Standard was issued pursuant to that direction, which sought to standardize the gathering, documenting, processing, analyzing, and sharing of Suspicious Activity Reports (SARs) among all levels of government through the NSI. I have participated in the development of each of the three versions of the Functional Standard (Versions 1.0, 1.5, 1.5.5) that have been issued to date.

3. The NSI seeks to build on the long-standing practice of state and local law enforcement collecting tips and leads and sharing them among one another and with the Federal government. Consistent with the IRTPA, 6 U.S.C. § 485(f)(2)(B), the White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005), A.R. at 1–5, and direction from the DNI, PM-ISE used a collaborative process in developing the Functional Standard.[1] PM-ISE routinely sought input from NSI participants at the Federal, state,

[1] Citations to the Administrative Record, ECF Nos. 53, 79–1, 79–2, are abbreviated "A.R." and citations to Supplemental Administrative Record, ECF No. 107, are abbreviated "Suppl. A.R." Citations to the A.R. include two documents that were inadvertently omitted from the initial Administrative Record, ECF No. 79-1, and corrected versions of six pages from the initial

and local levels, as well as advocates from organizations that promote civil liberties and privacy protections. PM-ISE considered collaboration to be an important step towards the development and implementation of a "decentralized, distributed, and coordinated" Information Sharing Environment (ISE), as described by the IRTPA. *See* 6 U.S.C. § 485(b)(2).

4. Additionally, the ISE standards must "take into account the varying missions and security requirements of ISE participants" and "address and facilitate information sharing between ISE mission partners." *See id.* at § 485(f)(2)(B) (i) & (v). In the NSI, the missions and authorities of NSI partners at Federal, State, and local levels of government are varied, with information sharing occurring between and among partners from different communities of interest (*e.g.*, law enforcement, homeland security, intelligence, and defense). The complexity of this initiative underscored the need for collaboration. Coordination and consultation helped frame the operational challenges and paved the way for the establishment of an effective national capacity for gathering, documenting, processing, analyzing, and sharing SAR information to prevent terrorism and other related criminal activity. *See id.* at § 485(f)(2)(B)(i), (iv), (v), & (vi).

5. In addition, the December 16, 2005 White House Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment (December 16, 2005) also contemplated collaboration. In addressing Guideline 2 (Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector), the Memorandum recognized that: "[The] war on terror must be a national effort [and as such] State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE, to the extent consistent with the applicable laws and executive orders and directives, the protection of national security, and the protection of the information privacy rights and other legal rights of Americans." A.R. at 2. As full partners and through collaboration, mission partners from various communities and differing levels of government identified operational

---

Administrative Record that were inadvertently reduced in size from the original or contained inadvertent redactions, ECF No. 79-2.

challenges, framed appropriate mission processes, and put in place protections appropriate for a coordinated approach to information sharing and safeguarding.

6. PM-ISE issued Functional Standard 1.0 on January 25, 2008. A.R. at 75–106. It was provided to the heads of all federal departments and agencies by memorandum, A.R. at 71–106, and made available to the public via the internet at www.ise.gov. As a matter of practice, PM-ISE posted documents of this type on or shortly after the issuance of the document, in order to ensure transparency. Functional Standard 1.0 also indicated that PM-ISE would periodically issue new or modified versions of the Functional Standard. A.R. at 77.

7. Following the issuance of Functional Standard 1.0, PM-ISE informed numerous groups that it intended to update this standard. To ensure that the public interest was represented in the updating process, PM-ISE solicited inputs and commentary from those groups.

8. PM-ISE held meetings with representatives of NSI participants at all levels of government, as well as with representatives of numerous privacy and civil liberties organizations. Among others, these organizations included the American Civil Liberties Union (ACLU), the Muslim Public Affairs Council; the Muslim Advocates, the Center for Democracy and Technology (CDT), the American-Arab Anti-Discrimination Committee, the Islamic Shura Council of Southern California, American Probation and Parole Association, state and local law enforcement agencies from various states (Pennsylvania, Minnesota, Georgia, New Jersey, Seattle, Iowa), the Department of Homeland Security, the Office of the Director for National Intelligence, and the Department of Justice. *See, e.g.*, A.R. at 116–119. On September 3, 2008, for example, the Office of PM-ISE hosted a Dialogue on Privacy and Civil Liberties that provided numerous groups, including those named above, the opportunity to discuss their privacy and civil liberties perspectives on the SAR process and to offer recommendations regarding the policies and safeguards that should be implemented. A.R. at 114–115, 120.

9. An additional "feedback session" with privacy and civil liberties advocates was held on February 18, 2009 and included representatives from many of the same organizations as those in

attendance at the September 2008 meeting, as well as representatives from the American-Arab Anti-Discrimination Committee, the Electronic Privacy Information Center (EPIC), and the Freedom and Justice Foundation. A.R. at 175–177.

10. PM-ISE also received oral and written input from numerous groups in response to its request for informal comments on possible amendments to Functional Standard 1.0. On January 23, 2009, for example, a representative of the ACLU sent an email to PM-ISE making a variety of suggestions for updating Functional Standard 1.0. A.R. at 158–60. Among other things, the ACLU representative stated that the definition of suspicious activity as "behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention" was likely to lead to the over-collection of information and suggested that the definition be amended to read as follows, "behavior reasonably indicative of pre-operational planning related to terrorism and other criminal activity." *Id.* at 158.

11. After reviewing all comments received, PM-ISE issued Functional Standard 1.5 on May 21, 2009. A.R. at 192–227. Functional Standard 1.5 was made available to the public by posting it on www.ISE.gov and www.ncirc.gov, by disseminating it via email to the NSI sites participating in the ISE-SAR Evaluation Environment (ISE-SAR EE), and by announcing it via an ACLU news release dated May 22, 2009. Functional Standard 1.5 again indicated that PM-ISE would periodically issue new or modified versions of the Functional Standard. *Id.* at 194.

12. PM-ISE also provided an explanation of the changes made to the Functional Standard. In particular, PM-ISE provided a memorandum to Federal departments and agencies regarding Functional Standard 1.5. A.R. at 187–88. That memorandum indicated that Functional Standard 1.5 incorporated several suggestions provided by Federal privacy and civil liberties attorneys and members of privacy and civil liberties organizations. At the suggestion of the ACLU, the definition of suspicious activity was refined to read as follows, "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." A fact-sheet announcing Functional Standard 1.5 and its changes from Functional Standard 1.0 was also made publicly available by posting it on

www.ISE.gov and by sending it to the ISE-SAR EE participating sites via email on or shortly after May 22, 2009. *Id.* at 189–90.

13. Following the issuance of Functional Standard 1.5, numerous groups were again informed that the Functional Standard was going to be updated and that they would be provided an opportunity to comment on issues related to that update. As it did when contemplating changes to Functional Standard 1.5, PM-ISE sought input from organizations dedicated to the preservation of privacy and civil liberties. On May 30, 2013, PM-ISE hosted an ISE Privacy, Civil Rights, and Civil Liberties Roundtable that provided numerous groups the opportunity to discuss their privacy and civil liberties perspectives on the SAR process and offer recommendations regarding the policies and safeguards that should be implemented. A.R. at 320–29. Among others, participating organizations included the ACLU, the Electronic Privacy Information Center, the CDT, the Constitution Project, the NYU Brennan Center, Muslim Advocates, the American-Arab Anti-Discrimination Committee, the Muslim Public Affairs Council, the Bill of Rights Defense Committee, the Leadership Conference on Civil and Human Rights, ODNI, the Department of Homeland Security, the Department of Justice, the NSI Office of the Program Manager, and various state or local law enforcement agencies, as well as organizations affiliated with state and local law enforcement.

14. In addition, in 2012, PM-ISE engaged in one-on-one sessions with privacy and civil liberties advocates to discuss issues of importance to all parties. *See, e.g.*, A.R. at 302–305 (Meeting between ACLU representative and PM-ISE), A.R. 306–307 (Meeting between EPIC representative and PM-ISE), A.R. at 308-313 (Meeting between The Constitution Project representative and PM-ISE), A.R. at 314-319 (Meeting between CDT representative and PM-ISE).

15. Finally, PM-ISE also received oral and written input on possible amendments to Functional Standard 1.5. For example, on September 19, 2013, twenty-seven privacy and civil liberties organizations sent a letter to Federal government officials (including PM-ISE) providing comments on Functional Standard 1.5 and suggesting changes for the next version of the Functional Standard. A.R. at 330–35. Among other things, the letter requested that the Functional Standard adopt the

"reasonable suspicion" standard articulated in 28 C.F.R. Part 23. *Id* The letter noted that that the organizations appreciated "the engagement with privacy and civil liberties organizations that the NSI and ISE have conducted in the past." *Id.* at 333.

16. After reviewing all comments received, PM-ISE issued Functional Standard 1.5.5 on February 23, 2015. A.R. at 414–473. Functional Standard 1.5.5 was made available to the public by posting on www.ISE.gov on February 23, 2015.

17. PM-ISE also provided an executive summary to explain the changes in the Functional Standard 1.5.5. A.R. at 338–45. The summary was provided to the President of the National Network of Fusion Centers and the Chair of the Criminal Intelligence Coordinating Council on November 21, 2014. A.R. at 335–405. It described the updating process, summarized the key changes that were incorporated into Functional Standard 1.5.5, and set forth a summary of the proposals which were not incorporated into the Functional Standard and the reasons for their exclusion. *Id.* Among other things, that summary also addressed the request by civil liberty and privacy advocates that the Functional Standard adopt the "reasonable suspicion" standard articulated in 28 C.F.R. Part 23 and the reasons why that standard was not adopted. *Id.* A March 2, 2015 blog posting at www.ise.gov also announced the issuance of Functional Standard 1.5.5 and summarized the changes from Functional Standard 1.5 to 1.5.5. A.R. at 474.

I certify under penalty of perjury that the foregoing is true and accurate. Executed in Washington, D.C. on August 17, 2016.

Basil N. Harris
Chief of Staff
Office of the Program Manager for the Information Sharing Environment, Office of Director of National Intelligence

EXHIBIT B

BENJAMIN C. MIZER
Principal Deputy Attorney General
ANTHONY J. COPPOLINO
Deputy Branch Director
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) 353-4556
Facsimile: (202) 616-8460
E-mail: kieran.g.gostin@usdoj.gov

Attorneys for Federal 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) (KAW)

DECLARATION OF MARILYNN B. ATSATT

I, Marilynn B. Atsatt, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I am Deputy Chief Financial Officer for the Office of Justice Programs (OJP), and have held that position since February 23, 2015. I am executing this declaration in support of the Government's motion for summary judgment in this case. The Office of the Chief Financial Officer's mission is to provide timely, accurate, and useful information; fiscal guidance; and fiduciary oversight ensuring financial integrity in support of the OJP's mission.

2. Among other things, the OJP is responsible for awarding and overseeing federal grants for the implementation of crime fighting technologies and strategies by state and local governments, including federal grants provided under the Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act), Pub. L. 90-351, 82 Stat. 197, codified at 42 U.S.C. § 3711 *et seq.* No other federal agency is responsible for awarding or overseeing federal grants under the Omnibus Act. Pursuant to its authority under that statute, *see* 42 U.S.C. § 3789g(c), the OJP issued 28 C.F.R. Part 23, a federal regulation governing the collection, maintenance, and dissemination of criminal intelligence in "criminal intelligence systems" that operate through support of the Omnibus Act. The OJP is responsible for enforcing that regulation.

3. I requested a review of all financial obligation records, including reimbursable agreements and grants, in the OJP's systems from January 2008 (the date I have been informed that the Functional Standard for the Information Sharing Environment, Suspicious Activity Reporting, Version 1.0, was released) until the present. Based on the results of that review provided to me, I have determined that the OJP has not provided any funding to the Federal Bureau of Investigation (FBI) for eGuardian or the NSI SAR DATA Repository. Accordingly, based on a review of the relevant records provided to me and my overall knowledge of the OJP's federal grant operations, I have determined that no Omnibus Act funding has been provided to the FBI for eGuardian or the NSI SAR Data Repository.

I certify under penalty of perjury that the foregoing is true and accurate. Executed in Washington, D.C. on August 18, 2016.

Marilynn B. Atsatt

Marilynn B. Atsatt
Deputy Chief Financial Officer