No. 17-16107

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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

Plaintiffs-Appellants,

v.

U.S. DEPARTMENT OF JUSTICE; JEFFERSON B. SESSIONS III, in his official capacity as Attorney General; PROGRAM MANAGER—INFORMATION SHARING ENVIRONMENT; and THE OFFICE OF PROGRAM MANAGER FOR THE INFORMATION SHARING ENVIRONMENT,

Defendants-Appellees.

On Appeal from the United States District Court for the Northern District of California, Case No. 3:14-cv-03120-RS

ANSWERING BRIEF FOR THE FEDERAL DEFENDANTS

CHAD A. READLER
Acting Assistant Attorney General

ALEX G. TSE
Acting United States Attorney

H. THOMAS BYRON III
(202) 616-5367
DANIEL AGUILAR
(202) 514-5432
Attorneys, Appellate Staff
Civil Division, Room 7266
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Cases: **Page(s)**

Statutes:

Rules:

Regulations:

Other Authorities:

GLOSSARY

ISE	Information Sharing Environment
ISE-SAR	Suspicious Activity Report shared in the Information Sharing Environment, through the NSI SDR
NSI	Nationwide Suspicious Activity Reporting Initiative
NSI SDR	NSI Suspicious Activity Report Data Repository
SAR	Suspicious Activity Report

STATEMENT OF JURISDICTION

The district court had jurisdiction under 28 U.S.C. §§ 1331, and entered summary judgment for the federal defendants on March 29, 2017. ER16. Plaintiffs filed a notice of appeal from that judgment on May 28, 2017. ER11-12. This Court has jurisdiction under 28 U.S.C. § 1291.

INTRODUCTION AND STATEMENT OF THE ISSUES

One of the critical lessons learned from the terrorist attacks of September 11, 2001, was that government agencies failed to effectively share information related to the attack before it happened. As a result, the agencies were not in the best position possible to identify, disrupt, warn against, or prevent the attacks. In the years that followed, both Congress and the President directed the federal government to create a system by which federal, local, state, and tribal agencies could share reports of suspicious activities that may be connected to terrorist threats. This system—the Information Sharing Environment—would allow law enforcement and national security agencies to aggregate information and be in the best position possible to "connect the dots" and identify terrorist threats before an attack could be carried out.

To help law enforcement agencies evaluate reports of suspicious activity and to create a uniform standard for determining what qualifies as potential terrorist activity, the federal government issued a "functional standard" to guide agencies in determining how to document, analyze, and share reports of suspicious activities. The functional standard was created through a collaborative process, in which the federal

government consulted with law enforcement agencies—and with privacy and civil-liberties groups—to ensure that the functional standard guided agencies to share high quality information about suspicious activity potentially related to terrorism, while it simultaneously protected individual people's constitutional and privacy rights. As part of this collaborative process, the federal government adopted the ACLU's proposal that "suspicious activity" should be defined as "behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." SER346; ER504.

Plaintiffs have brought a challenge to the functional standard under the Administrative Procedure Act, arguing that the functional standard is a legislative rule that ought to have been submitted for notice and comment, and that the functional standard's definition of "suspicious activity" is unlawful and inconsistent with particular regulations promulgated by the Department of Justice. The district court granted summary judgment to the federal defendants, holding that the functional standard was not a legislative rule, and that the definition of "suspicious activity" was appropriate and consistent with the Department's regulations.

The issues presented on appeal are:

1. Have the plaintiffs challenged final agency action within the meaning of the Administrative Procedure Act?

2. Is the functional standard a legislative rule that must go through public notice and comment before it may be implemented?

3. Is the functional standard arbitrary and capricious because it permits agencies to share information that is "reasonably indicative of pre-operational planning associated with terrorism or other criminal activity," rather than only permitting agencies to share information that satisfies the "reasonable suspicion" standard contained in 28 C.F.R. Part 23 for sharing criminal intelligence information?

PERTINENT STATUTES AND REGULATIONS

Per Ninth Circuit Rule 28-2.7, an addendum of pertinent statutes and regulations appears at the end of this brief.

STATEMENT OF THE CASE

I. BACKGROUND AND LEGAL FRAMEWORK OF THE FUNCTIONAL STANDARD FOR SHARING SUSPICIOUS ACTIVITY REPORTS

A. September 11th and the Need to Share Information About Terrorism

On September 11, 2001, terrorists hijacked four aircraft and used them to attack the World Trade Center and the Pentagon. As part of the overall national response to September 11th, Congress established a commission to "examine and report upon the facts and causes" of these terrorist attacks, and to report "findings, conclusions, and recommendations for corrective measures that can be taken to prevent acts of terrorism." Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, § 602, 116 Stat. 2383, 2408 (2002). In its final report, the commission noted that there were "missed opportunities to thwart the 9/11 plot," because "[i]nformation was not shared, sometimes inadvertently or because of legal

misunderstandings. Analysis was not pooled. Effective operations were not launched." *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* 353 (2004), https://go.usa.gov/xn6VH. One of the clear lessons of the September 11th attacks is that the United States must collect "information about terrorist risks and threats and then ensur[e] that the information gets into the hands of those whose responsibility it is to protect our communities and critical infrastructure." SER23.

Shortly after the commission's report, the President issued an executive order directing the federal government to create a "terrorism information sharing environment" that would help government agencies share information in order to detect, disrupt, and prevent terrorist threats. Executive Order 13,356, 69 Fed. Reg. 53,599, 53,600 (Aug. 27, 2004). Congress largely codified this executive order and directed the President to "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." 6 U.S.C. § 485(b)(1)(A); *see also id.* § 481(b)(10) (federal, state, and local governments must "act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks"). This information sharing environment (ISE) is a decentralized system that allows federal, state, local, and tribal governments to connect to each other and share information for analysis "without the need to centralize information." *Id.* § 485(b)(2)(L).

To oversee the ISE's operations, Congress created the office of Program Manager for the Information Sharing Environment. 6 U.S.C. § 485(f). The Program Manager is responsible for, among other things, issuing "governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE." *Id.* § 485(f)(2)(A)(iii).

B. Suspicious Activity Reports (SARs)

Building on this legal framework, the President issued a national strategy for sharing terrorism-related information. SER11-58. The strategy called for effective sharing of information among federal agencies and with the "Nation's first 'preventers and responders'"—the state, local, and tribal governments that are "often best able to identify potential threats that exist within their jurisdictions." SER19. To accomplish this, the President called for a "unified process" to report, process, and access locally generated information regarding "suspicious incidents, events, and activities." SER54. These suspicious activity reports (SARs) should be "disseminated to and evaluated by appropriate government authorities." SER55. By September 2007, state and local governments had created fifty-eight "fusion centers," centers staffed by trained analysts who can gather, analyze, and share SARs related to terrorism. SER24. This nationwide effort to share SARs related to terrorism is known as the Nationwide Suspicious Activity Reporting Initiative (NSI). ER503.

SARs typically originate from a law enforcement officer or private citizen who has observed suspicious activity and reported it for an initial investigation or fact

gathering. ER513, 558. The investigating officer may then document the activity as a SAR, which is then further reviewed by officials at an appropriate federal, state, local, tribal, or territorial law enforcement agency to determine whether to send the SAR to a fusion center or FBI field office. ER513-14, 558. After a trained analyst at the fusion center or field office vets the SAR to confirm that it has a potential nexus to terrorism, the SAR is submitted to the NSI SAR Data Repository (NSI SDR), where it can be shared with other law enforcement and homeland security agencies participating in the NSI. ER514-15.[1] A SAR that has gone through all these layers of review, determined to have a potential nexus to terrorism, and shared with other NSI participants is called an ISE-SAR. ER514.

C. The Development of the Functional Standard for Sharing SARs

Because many law enforcement agencies across the country used a variety of different methods for documenting and sharing SARs, including SARs related to terrorism, the Program Manager for the ISE issued a common standard—the functional standard—to "govern[] how terrorism information is acquired, accessed, shared, and used within the ISE." ER397. The Program Manager has issued three Functional Standards, which have superseded each other: Functional Standard 1.0 (issued January 2008), ER397-432; Functional Standard 1.5 (issued May 2009), ER448-85; and Functional Standard 1.5.5 (issued February 2015), ER501-60. Unless

[1] The NSI SDR is housed within eGuardian, the FBI's unclassified, Web-based system for receiving, tracking, and sharing SARs in the NSI. ER3, 493, 502.

otherwise noted, this brief refers to the currently-operative Functional Standard 1.5.5 as "the functional standard." At issue in this case is the functional standard's definition of "suspicious activity" and its standards for processing and sharing suspicious activity reports.

1. Functional Standard 1.0

Functional Standard 1.0 defined suspicious activity as "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention." ER406. It listed eighteen different categories of preoperational behaviors that could have a potential nexus to terrorism, such as attempting to gain unauthorized access to restricted areas; making threats to damage or compromise infrastructure; acquiring unusual amounts of precursor materials that could be used for terrorism; photographing infrastructure and personnel; and similar activities. ER427. An analyst at a fusion center or federal agency would review a SAR, determine whether the reported information had a potential nexus to terrorism and, if so, share the SAR through ISE Shared Spaces (a forerunner to the current method of sharing through the NSI SDR). ER408-09. The Program Manager made Functional Standard 1.0 available to the public by publishing it online. SER8.

2. Developing Functional Standard 1.5

After issuing the initial functional standard (Functional Standard 1.0), the Program Manager notified government agencies and non-governmental organizations

that he intended to revise the functional standard and sought advice and comments from these groups. SER8. The Program Manager hosted a conference concerning "Dialogue on Privacy and Civil Liberties," SER304-10, to discuss potential issues with SARs and Functional Standard 1.0 with advocates from the ACLU, the Muslim Public Affairs Council, the Center for Democracy and Technology, and the American-Arab Anti-Discrimination Committee (among others), SER306-08.

Following this conference, the ACLU expressed concern that Functional Standard 1.0's criteria for determining what constituted suspicious activity was unnecessarily broad and would cause law enforcement to investigate innocent persons who might then be documented in a SAR. SER346. In particular, the ACLU was concerned that Functional Standard 1.0's definition of suspicious activity—"behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention"—was vague, overbroad, and "disconnected from an appropriate legal standard." *Id.* Instead, the ACLU "suggest[ed] amending the definition of a SAR to '*behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity*.'" *Id.* (emphasis added). The Program Manager adopted the ACLU's proposed definition of suspicious activity for both Functional Standard 1.5 (ER451) and Functional Standard 1.5.5 (ER504).[2]

[2] The ACLU also recommended clarifying that some potentially suspicious activities may nevertheless be protected by the First Amendment, and that race and religion should not be considered independent factors that could create reasonable

The Program Manager then held another conference to solicit comments from privacy and civil-liberties advocates about the Functional Standard and the training for line-officers involved with SARs. SER363. This conference included many of the same groups that attended the previous conference, such as the ACLU, the Freedom and Justice Foundation, Muslim Advocates, and EPIC (Electronic Privacy Information Center), along with many federal, state, and local agencies. SER364-65. After the conference, an ACLU representative sent an email to say thanks "for inviting me up to talk about the new draft functional standards." SER370. The ACLU representative then offered a comment to clarify the Functional Standard's definition of suspicious activity—that "intelligence gathering" should not be distinguished from "pre-operational planning." SER370. This suggestion was adopted and incorporated into Functional Standard 1.5 and Functional Standard 1.5.5. ER451, 504.

3. Functional Standard 1.5

After this collaborative effort to revise the initial functional standard, the Program Manager issued Functional Standard 1.5 on May 21, 2009. ER450-53. The

---

suspicion. SER347. The ACLU further recommended discussing stop-and-frisk standards under *Terry v. Ohio*, and clarifying that additional information may be necessary to determine whether a limited investigation has identified sufficiently suspicious activity that should be included in a SAR. *Id.* These recommendations were accepted and implemented in Functional Standard 1.5 (ER456, 458) and Functional Standard 1.5.5 (ER510-11, 513).

revised standard defined suspicious activity as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." ER455. It also listed seven criminal activities that had a potential nexus to terrorism (*e.g.*, sabotage, cyber attacks, express or implied threats to damage or compromise infrastructure), and eight activities that are potentially criminal or potentially non-criminal, and which would require further fact development to determine if they met the definition of suspicious activity (*e.g.*, asking questions about a building's security procedures, photographing infrequently used entrances to facilities, training in military tactics and weapons). ER478-79. Functional Standard 1.5 made it clear that many activities are constitutionally protected and should not be considered suspicious "absent articulable facts and circumstances" that they are criminal activity related to terrorism. ER478 n.11. It further stressed that a person's race, ethnicity, national origin, or religion "should not be considered as factors that create suspicion (except if used as part of a specific suspect description)." ER456.

The day after Functional Standard 1.5 was issued, the ACLU issued a press release stating that these revisions "give law enforcement the authority it needs without sacrificing the rights of those it seeks to protect." ACLU, *Intelligence Community Raises Its Standards For Information Collection: Collaborative Effort Addresses Privacy and Civil Liberties Concerns* (May 22, 2009), https://www.aclu.org/print/node/14071; *see also id.* ("We hope other agencies will adopt these reasonable and constitutional standards to govern their own information collection.").

4. Further Collaboration and Functional Standard 1.5.5

A year after Functional Standard 1.5 was issued, the Program Manager drafted a report advising NSI participants of policies and best practices to safeguard people's privacy and civil liberties while still effectively sharing suspicious activity reports. SER409-45. Before the report was finalized, the ACLU had an opportunity to edit and comment on a draft of the report. SER301 (Doc.29), SER373-408. The ACLU's edits compared Functional Standard 1.0 to Functional Standard 1.5, commenting that while Functional Standard 1.0 allowed SARs to be based on "mere suspicion," the "reasonably indicative" language in Functional Standard 1.5 gives law enforcement officers "a standard of review that will result in better quality SARs * * * while, at the same time, enhancing privacy protections." SER386 & n.18. The ACLU wrote that the higher "reasonably indicative" standard "produces sufficiently high quality information to enable agencies and analysts to 'connect the dots.'" SER387; *see also* SER424-26 (final version of this report).

Throughout 2012, the Program Manager met with members of non-governmental organizations and advocacy groups to discuss the operation of the ISE and any concerns about privacy and civil liberties. SER446-55. In 2013, the Program Manager held another conference with these groups and with federal, state, and local agencies to discuss ISE issues and the functional standard. SER456-60.

In 2015, the Program Manager issued Functional Standard 1.5.5, which continued to define suspicious activity as "[o]bserved behavior reasonably indicative

of pre-operational planning associated with terrorism or other criminal activity." ER504, 506. Like the previous functional standard, it also listed seven criminal activities that had a potential nexus to terrorism (*e.g.*, death threats, sabotage of secured sites) and nine potentially criminal or non-criminal activities that would require additional information to determine whether they met the definition of suspicious activity (*e.g.*, collecting unusual amounts of weapons). ER541-51.

The functional standard explained that once there has been a report of suspicious activity, the law enforcement agency responding to that report should document the behavior in a SAR in accordance with Functional Standard 1.5.5. ER513. That agency should then send that SAR to a fusion center or FBI field office (as appropriate) for further review to determine "whether the SAR reflects" one of the listed criminal or non-criminal activities that may have a potential nexus to terrorism. *Id.* If it does, the trained analyst reviewing the SAR next applies "his or her professional judgment to determine whether, based on the available context, facts, and circumstances, the information has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism)." ER514. If there is a potential nexus to terrorism, then it is an ISE-SAR and should be shared through the NSI SDR with all NSI participants (federal, state, local, and tribal government agencies). ER514-15.

Functional Standard 1.5.5 also called for analysts and investigators to communicate with each other about whether a SAR actually reported suspicious

activity. For example, if a fusion center determines that a SAR has a potential nexus to terrorism and should be shared through the NSI SDR, the fusion center should notify the source agency (the agency that originally documented the SAR) so that "organizations know that their initial suspicions have some validity." ER515. And when the FBI investigates that particular ISE-SAR, the FBI should notify the fusion center of the investigation and its results. *Id.* Through these multiple levels of review and analysis, the functional standard seeks to filter out SARs that lack a potential nexus to terrorism from being shared through the NSI SDR "to the maximum extent possible." *Id.*

Functional Standard 1.5.5 is "focused exclusively on terrorism-related information." ER516. Agencies participating in the NSI may still share information outside of the NSI SDR, but that sharing still "must be done in accordance with other agency legal authorities, policies and procedures, and interagency agreements." ER517.

D. The Functional Standard's Relationship with 28 C.F.R. Part 23

Separate from the ISE and NSI, and pursuant to different statutory authority, the Department of Justice has issued regulations designed to "assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968 [(Omnibus Crime Control Act)] are utilized in conformance with the privacy and constitutional rights of individuals." 28 C.F.R. § 23.1 (citations omitted). These regulations in 28 C.F.R. Part 23 govern the

investigation and "exchange of intelligence data" of "ongoing networks of criminal activity" that participate in crimes such as "loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials." *Id.* § 23.2. Systems that collect and store this kind of criminal intelligence information "concerning an individual" may only do so "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). "Reasonable [s]uspicion" exists when there are "sufficient facts to give a trained law enforcement or criminal investigative agency officer * * * a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise." *Id.* § 23.20(c). These regulations apply to "all criminal intelligence systems" that are funded under the Omnibus Crime Control Act, *id.* § 23.3(a), which provides funds to state and local governments, *Tafoya v. U.S. Dep't of Justice*, 748 F.2d 1389, 1390-91 (10th Cir. 1984).

Both before and after the implementation of the Functional Standard 1.0, the Department of Justice and the Program Manager expressed their view that suspicious activity reports shared through the NSI SDR are not generally governed by 28 C.F.R. Part 23, because these do not qualify as criminal intelligence information but instead concern potential terrorism threats. In 2007, the Department of Justice issued a report concerning "Tips and Leads" including "suspicious activity reports (SARs)." SER350, 356. At the outset, the report explained that "[t]ips and leads data are not

criminal intelligence as defined by 28 Code of Federal Regulation (CFR) Part 23," SER351, and explicitly distinguished the two categories, SER352. The report went on to explain that both categories of information need to be shared with federal, state, local, and tribal governments to ensure that those entities "have access to timely, credible, and actionable information and intelligence regarding individuals and groups intending to carry out attacks within the United States." SER353.[3]

In the fall of 2008, the Program Manager (in consultation with the Department of Justice) issued a report noting that there might be occasions when a SAR falls under Part 23's requirements. ER433-34, 440. However, ISE-SARs shared through the NSI SDR are generally "considered fact-based information rather than criminal intelligence" information subject to Part 23 (ER440), and the Program Manager recommended that agencies participating in the NSI should "clearly articulate when 28 CFR Part 23 should be applied" (ER446). Around the same time, the Department of Justice issued a separate report that outlined when an ISE-SAR may become subject to Part 23's regulations. ER272, 288-89. If a SAR meets the functional standard's criteria and has a potential nexus to terrorism, it may be shared with NSI participants through ISE Shared Spaces (a forerunner to the NSI SDR). ER289. If the information in the SAR separately establishes reasonable suspicion, then that

[3] This report was shared with the ACLU as part of the collaborative discussion to develop Functional Standard 1.5. SER349.

information may be separately shared as criminal intelligence information subject to Part 23. *Id.*

In January 2009, shortly before Functional Standard 1.5 was issued, the Department of Justice and the Program Manager issued guidance to help NSI participants implement "ISE-SAR Shared Spaces," a platform that would allow participants more efficient access to ISE-SARs. SER59, 63. That guidance noted that the Shared Spaces platform that accesses ISE-SARs "is not a criminal intelligence system or database that would require application of 28 CFR Part 23." SER68. However, once "SAR data rises to the level of reasonable suspicion," it should also be submitted "to a criminal intelligence information database or system." SER69.

During the development of Functional Standard 1.5, at least one civil-liberties advocate commented that the government should "reconsider" its position that "SARs do not qualify as 'criminal intelligence investigation'" under 28 C.F.R. Part 23. SER367. The government did not change its position, and reiterated that it had discussed the "reasonably indicative standard" with "project participants, legal experts, and representatives of privacy advocacy groups," and determined that this was the correct "level of suspicion" for sharing SARs. SER138. *See also* SER247 (if and when the information in a SAR "rises to the level of reasonable suspicion" then the information could be submitted to "an intelligence database").

The Program Manager incorporated this interpretation of Part 23 into Functional Standard 1.5.5. A suspicious activity report shared through the NSI SDR

"may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23." ER555. The Program Manager explained that ISE-SARs "represent[] information about suspicious behavior" that has a potential nexus to terrorism, while criminal intelligence information focuses on "the specific criminal subject(s), the criminal activity in which they are engaged, and the evaluation of facts to determine that the reasonable suspicion standard has been met." ER500.

II. PRIOR PROCEEDINGS

Plaintiffs, represented by the ACLU, filed a complaint raising two challenges to the functional standard.[4] First, plaintiffs alleged that the functional standard was a legislative rule and should have been promulgated under the notice and comment procedures in 5 U.S.C. § 553. SER294-95, 496. Second, they alleged that the "reasonably indicative" standard for sharing SARs was arbitrary, capricious, and

[4] The complaint named as defendants two agencies (the Department of Justice and the Program Manager—Information Sharing Environment) and two individuals in their official capacity (Attorney General Eric H. Holder, Jr., and Program Manager Kshemendra Paul). SER461, 465-66. Attorney General Jefferson B. Sessions III has been substituted for Attorney General Holder. Fed. R. Civ. P. 25(d); Fed. R. App. P. 43(c)(2). Program Manager Paul resigned from his position in 2017, and the office is currently vacant. The Office of Program Manager has been listed as the defendant-appellee in the caption to this brief. Fed. R. Civ. P. 17(d); Fed. R. App. P. 43(c)(1).

otherwise not in accordance with law because it was inconsistent with 28 C.F.R. Part 23. SER292-94, 494-95.[5]

The district court denied defendants' motion to dismiss, holding, *inter alia*, that the functional standard was final agency action that could be challenged under 5 U.S.C. § 704 (ER576-77), and that plaintiffs' claims concerning notice and comment and the applicability of Part 23 would likely involve factual disputes and could not be resolved on a motion to dismiss (ER577-79).

After the parties filed cross-motions for summary judgment, the district court granted judgment to the federal defendants. ER2. First, the court concluded that the functional standard was not a legislative rule that "create[s] rights, impose[s] obligations, or effect[s] a change in existing law." ER5 (quoting *Hemp Indus. Ass'n v. DEA*, 333 F.3d 1082, 1087 (9th Cir. 2003)). Instead, the court explained, the functional standard is "an operating procedure—a policy, a plan, a strategy—allowing cooperation and communication among various governmental actors." ER5. Because the functional standard "merely provides guidance" rather than imposing legal obligations and consequences, it was not a legislative rule and was not required to be submitted for notice and comment under 5 U.S.C. § 553(b). ER5. The court

[5] Although the complaint and the first amended complaint alleged that the Department of Justice and the Program Manager had promulgated different functional standards, by summary judgment the parties agreed that plaintiffs were challenging the current Functional Standard 1.5.5 and the earlier Functional Standard 1.5. ER3.

further noted that while it had previously concluded (in denying the motion to dismiss) that the functional standard was final agency action, that conclusion may have been wrong because there was "good reason to treat the Functional Standard as not constituting a final agency action within the meaning of *Bennett v. Spear* [520 U.S. 154, 177-78 (1997)]." ER6.

Next, the court held that the functional standard was not arbitrary and capricious for allowing ISE-SARs to be shared if they contained information that was "reasonably indicative of pre-operational planning associated with terrorism or other criminal activity." ER7-10, 504, 509. While this standard was different from the standard set forth in 28 C.F.R. Part 23, those regulations only govern systems for storing and distributing "criminal intelligence [information]," and the ISE-SARs shared through the NSI SDR are not "criminal intelligence [information]." ER8-9. Because the functional standard addresses "data collection and dissemination issues not already within the scope of Part 23," it was not arbitrary and capricious for the functional standard to be different than 28 C.F.R. § 23.20(a)'s "reasonable suspicion" standard. ER9.[6]

[6] Defendants proffered a declaration that certain federal information sharing systems are not funded under the Omnibus Crime Control Act and are exempt from the requirements of Part 23. ER9; *see also* 28 C.F.R. § 23.3(a). The district court struck that declaration and granted summary judgment to the defendants based solely on the administrative record, for the reasons described above. ER9-10.

SUMMARY OF ARGUMENT

I. The Administrative Procedure Act only permits challenges to final agency action, 5 U.S.C. § 704, meaning action that determines "rights or obligations" or "from which 'legal consequences will flow.'" *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997). Plaintiffs' challenge to the functional standard fails because the functional standard does not determine rights or obligations, nor does it impose legal consequences. Instead, the functional standard sets forth uniform guidelines for sharing suspicious activity reports with other governmental agencies. There are no legal consequences for violating the functional standard, and no legal mechanisms for enforcing it. While the functional standard has great practical value in ensuring that agencies collaborate with each other to share high quality information about potential terrorist threats, it does not qualify as final agency action under 5 U.S.C. § 704.

II. For similar reasons, the functional standard does not qualify as a substantive, legislative rule that must be promulgated through the notice-and-comment procedures in 5 U.S.C. § 553. The functional standard does not "create rights, impose obligations, or effect a change in existing law." ER5 (quoting *Hemp Indus. Ass'n v. DEA*, 333 F.3d 1082, 1087 (9th Cir. 2003)). Instead, the functional standard serves as a general statement of policy, setting forth best practices for how agencies should standardize their gathering, documenting, analyzing, and sharing of suspicious activity reports that have a potential nexus to terrorism.

Even if notice and comment were required, the record in this case demonstrates that plaintiffs did not suffer any prejudice. 5 U.S.C. § 706. The functional standard adopted the "reasonably indicative" standard suggested by the ACLU, and the agency considered many comments from privacy and civil-liberties advocates addressing how the functional standard could be designed to best protect people's privacy and constitutional rights. The functional standard adopted most of those suggestions outright, and plaintiffs do not identify any way in which broader notice and comment would have altered the process of developing the functional standard or the substance of the functional standard that the agency adopted.

III. The functional standard does not conflict with 28 C.F.R. Part 23, which requires "reasonable suspicion" before disseminating criminal intelligence information, because Part 23 does not generally apply to suspicious activity reports that are potentially related to terrorist threats. Rather, Part 23 applies to information concerning a specific individual or organization reasonably suspected of being involved in criminal activity. 28 C.F.R. § 23.3(b)(3)(i). It does not apply to reports of potential terrorist activity, which are not necessarily focused on identifying or investigating a particular individual or organization, and which need to be collected and analyzed in significant quantities in order to determine the nature of a potential terrorist threat. *See Hamdan v. U.S. Dep't of Justice*, 797 F.3d 759, 775 (9th Cir. 2015) ("[L]ike a piece of a jigsaw puzzle, [every detail] may aid in piecing together other bits of information even when the individual piece is not of obvious importance in

itself."). Plaintiffs' interpretation of the Part 23 regulations is directly contrary to the consistent interpretation of the Department of Justice, which promulgated those rules. The Department's interpretation of its own regulations is entitled to deference. *Auer v. Robbins*, 519 U.S. 452, 461 (1997).

STANDARD OF REVIEW

This Court reviews a grant of summary judgment de novo and may affirm on any ground supported by the record. *White v. City of Sparks*, 500 F.3d 953, 955 (9th Cir. 2007). Final agency action will be held unlawful if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. §§ 704, 706(2)(A). A violation of the Administrative Procedure Act is reviewed for harmless error. 5 U.S.C. § 706; *Shinseki v. Sanders*, 556 U.S. 396, 406-07 (2009).

ARGUMENT

I. THE FUNCTIONAL STANDARD IS NOT FINAL AGENCY ACTION UNDER THE ADMINISTRATIVE PROCEDURE ACT

Under the Administrative Procedure Act, plaintiffs may challenge the functional standard if it is a "final agency action." 5 U.S.C. § 704.[7] An agency's action is "final" if it meets a two-pronged test: First, the action must "mark the consummation of the agency's decisionmaking process," and second, it must be an action "by which rights or obligations have been determined, or from which legal

[7] Non-final agency action can also be reviewed under 5 U.S.C. § 704 if another statute explicitly permits judicial review, but plaintiffs have not argued that any other statute besides § 704 permits judicial review of the functional standard.

consequences will flow." *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997) (quotation marks omitted).

To determine whether the second prong has been met, this Court has considered whether the challenged action "has a direct and immediate effect on the day-to-day operations of the party seeking review, and whether immediate compliance [with the terms] is expected." *Industrial Customers of Nw. Utils. v. Bonneville Power Admin.*, 408 F.3d 638, 646 (9th Cir. 2005) (citing *FTC v. Standard Oil Co.*, 449 U.S. 232, 239-40 (1980)). If the action does not "impos[e] any obligation …, deny[] any right …, or fix[] any legal relationship," it does not qualify as final agency action. *Independent Equip. Dealers Ass'n v. EPA*, 372 F.3d 420, 427 (D.C. Cir. 2004) (Roberts, J.); *see also Ukiah Valley Med. Ctr. v. FTC*, 911 F.2d 261, 264 (9th Cir. 1990) (same). Notably, plaintiffs do not argue that the functional standard determines their own legal rights or obligations, or those of any regulated entity—rather, they argue that the functional standard determines the legal rights and obligations of government agencies that participate in the NSI. Opening Br. 40. But that very distinction demonstrates that the functional standard does not impose binding obligations. Participating government agencies voluntarily submit information by creating SARs, and choose to participate in the NSI to obtain and to share information relevant to their efforts to identify and deter terrorist threats. The functional standard merely provides procedural guidelines for that voluntary participation.

The functional standard does not qualify as final agency action because it does not impose obligations, deny any rights, or fix any legal relationship. The functional standard provides standardized guidance to agencies that choose to participate in the NSI, defining the factors they should consider when sharing suspicious activity reports through the NSI SDR. The functional standard calls on agencies to submit a SAR through the NSI SDR when it reflects suspicious behavior "reasonably indicative of pre-operational planning associated with terrorism or other criminal activity," and qualifies as an ISE-SAR ER509-15. There are no mechanisms for compelling an agency's adherence to the functional standard, nor are there any changes in an agency's legal relationship with the federal government if the agency submits a report to the NSI SDR that falls short of the reasonably indicative standard. Indeed, Congress directed that the ISE should be a "decentralized, distributed, and coordinated environment" that prevents any one actor from strictly controlling all of the information shared through it. 6 U.S.C. § 485(b)(2).

Many NSI participants may choose to follow the functional standard as a practical guide for sharing terrorism threats with other agencies. "But *de facto* compliance is not enough to establish that the" functional standard has "had *legal* consequences." *Center for Auto Safety v. National Highway Traffic Safety Admin.*, 452 F.3d 798, 811 (D.C. Cir. 2006). In *Center for Auto Safety*, the federal government issued guidelines for when a car manufacturer could issue a recall for specific regions of the country rather than a national recall. *Id.* at 803-04. While the guidelines certainly

reflected the government's view "on the legality of regional recalls," it did not determine any rights or obligations, nor did it have any legal consequences. *Id.* at 808. While the guidelines may "have become a *de facto* industry standard for how to conduct regional recalls," the government did not "coerce[]" or "force[]" manufacturers to abide by the guidelines. *Id.* at 811. And without a change in parties' "rights or obligations" or "*legal* consequences" to the parties, there is no final agency action. *See id.* (citing *Bennett*, 520 U.S. at 178).

As the Sixth Circuit has explained, actions that "legally bind an agency or prevent other government actors from pursuing a particular course of action cause legal consequences." *Parsons v. U.S. Dep't of Justice*, 878 F.3d 162, 167 (6th Cir. 2017). But "[o]ther *practical* results of an agency's action that lack similar immediate and significant effects are not legal consequences." *Id.* at 168 (emphasis added). This Court has similarly distinguished the "*legal* status" of an agency's action from its "*practical* effect[s]," and has cautioned against "erroneously conflat[ing]" the two when determining whether there is final agency action. *Fairbanks N. Star Borough v. U.S. Army Corps of Eng'rs*, 543 F.3d 586, 595 (9th Cir. 2008).

It is a practical benefit for all NSI participants to report and receive suspicious activity reports that meet the functional standard—these will be reports with a "sufficiently high quality of information" that enables "analysts to 'connect the dots' while not producing so much information as to overwhelm agency analytical capacity." ER491. But plaintiffs fail to identify any legal consequences that flow

from the functional standard. Both before and after the functional standard's issuance, an NSI participant may share a terrorism-related SAR with other law enforcement agencies when it believes it ought to do so. In other words, the functional standard "did not change the legal situation," and it does not qualify as final agency action. *International Bhd. of Teamsters v. U.S. Dep't of Transp.*, 861 F.3d 944, 952 (9th Cir. 2017); *see also Guerrero v. Clinton*, 157 F.3d 1190, 1195 (9th Cir. 1998) (a report was not final agency action because "it has no determinative or coercive effect upon the action of someone else" (quotation marks omitted)).

By contrast, all of the cases plaintiffs rely upon concern agency actions that altered the existing legal regime. In *Bennett*, the Fish and Wildlife Service issued a biological opinion that "sets forth the terms and conditions * * * that must be complied with by the Federal agency or applicant" for the incidental taking of an endangered species. 16 U.S.C. § 1536(b)(4)(iv); *see Bennett*, 520 U.S. at 158. The biological opinion thus imposed legal requirements and "alter[ed] the legal regime" under which another agency (the Bureau of Reclamation) could operate an irrigation project. *Bennett*, 520 U.S. at 178. If the Bureau failed to comply with the biological opinion, it would do so "'at its own peril,' since any person who knowingly takes an endangered species * * * is 'subject to substantial civil and criminal penalties.'" *San Luis & Delta-Mendota Water Auth. v. Salazar*, 638 F.3d 1163, 1170 (9th Cir. 2011) (quoting *Bennett*, 520 U.S. at 170).

The agency action in *Oregon Natural Desert Ass'n v. U.S. Forest Service*, 465 F.3d 977 (9th Cir. 2006), likewise had substantive legal effects. There, the Forest Service issued grazing permits to ranchers, allowing them to graze their livestock on federal land, and the permit included "annual operating instructions" that further specified how the rancher was permitted to use livestock on federal land. *Id.* at 979-80. If the rancher failed to follow those instructions, the Forest Service could "institute agency proceedings against" the rancher to change or suspend the rancher's permit. *Id.* at 987-88.

Plaintiffs do not identify any comparable, substantive legal requirements imposed by, or legal consequences that flow from, the functional standard. An agency that deviates from the functional standard does not lose access to ISE-SARs, nor is there any risk of enforcement proceedings, civil penalties, or criminal penalties. The functional standard does not create any enforceable legal rights or obligations for NSI participants. Instead, it sets forth a standard for sharing terrorism-related SARs, and many agencies voluntarily choose to comply with it as a practical matter because the functional standard articulates the best current practices for sharing information about suspicious activities that may indicate a potential terrorist threat.

Accordingly, the district court noted that "there is good reason to treat the Functional Standard as not constituting a final agency action," although its decision ultimately rested on the different but related conclusion that the functional standard is not a legislative rule. ER6. This Court, however, may affirm the district court's grant

of summary judgment on the alternative ground that the functional standard is not final agency action. *See Direct Technologies, LLC v. Electronic Arts, Inc.*, 836 F.3d 1059, 1071 (9th Cir. 2016) (affirming summary judgment on alternative grounds).

II. THE FUNCTIONAL STANDARD IS NOT A LEGISLATIVE RULE SUBJECT TO NOTICE AND COMMENT

A. The Functional Standard Does Not Create Rights, Impose Obligations, or Effect a Change in Existing Law

Under the Administrative Procedure Act, agencies generally must publish rules in the Federal Register to give the public an opportunity for notice and comment before the rule takes effect. 5 U.S.C. § 553. But an agency's "interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice" are exempted from this requirement, *id.* § 553(b)(A), and only an agency's legislative rules that "create rights, impose obligations, or effect a change in existing law" must follow notice and comment. ER5 (quoting *Hemp Indus. Ass'n v. DEA*, 333 F.3d 1082, 1087 (9th Cir. 2003)).

The district court correctly concluded that the functional standard is a general statement of policy, an "operating procedure" that allows "cooperation and communication among various governmental actors," reflecting when agencies participating in the NSI should share terrorism-related SARs. ER5. Relying on this Court's opinion in *Mada-Luna v. Fitzpatrick*, 813 F.2d 1006, 1013-14 (9th Cir. 1987), the district court determined that the functional standard "merely provides guidance to agency officials in exercising their discretionary powers." ER6. *See also Mada-Luna*,

813 F.2d at 1015 (a general statement of policy leaves officials "free to consider the individual facts in the various cases that arise and to exercise discretion") (quotation marks omitted).

For many of the same reasons that the functional standard does not qualify as final agency action, *supra* pp. 23-28, it also does not qualify as a legislative rule. The functional standard does not create rights, impose duties, or change existing law. *Hemp Indus. Ass'n*, 333 F.3d at 1087. Instead, it provides general, standardized guidance to agencies participating in the NSI. The functional standard begins by stating that it is "limited to describing the ISE-SAR process and associated information exchanges." ER501; *see also* ER504 (the functional standard is "[g]uidance" that "describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs"). It is designed to provide "a standardized means of identifying and sharing ISE-SARs and applying data analytic tools to the information." ER511. The functional standard makes clear that it "does not alter law enforcement officers' constitutional obligations when interacting with the public," and all applicable laws and regulations still apply when an officer takes action against a person—even when that action is potentially based on information from an ISE-SAR. ER510-11.

When a participating agency's analyst is determining whether to share a SAR, he or she must "apply his or her professional judgment to determine whether, based on the available context, facts, and circumstances, the information has a potential

nexus to terrorism." ER514. It is only after that use of professional judgment to evaluate a particular SAR that the analyst chooses whether to designate it as an ISE-SAR and share it through the NSI SDR, "where it is immediately provided to the FBI for an assessment-level investigation and made available to all other" participants. ER515. Throughout this process, the analyst "remains free to consider the individual facts in the various cases that arise," and accordingly the functional standard is not a "binding norm" that constitutes a legislative rule. *Ryder Truck Lines, Inc. v. United States*, 716 F.2d 1369, 1377 (11th Cir. 1983) (cited with approval in *Mada-Luna*, 813 F.2d at 1013-14).

Plaintiffs observe that the functional standard lists sixteen categories of potentially suspicious behavior (which have historically been associated with terrorism) that should be considered in determining whether to share an ISE-SAR through the NSI SDR. ER541-51. But even if a SAR reports activity that falls within one of those categories, that does not necessarily mean that the SAR reflects activity with a potential connection to terrorism—further individualized analysis is required. ER514. Nine of those categories involve behaviors that may be "constitutionally protected activities," and as such should only be documented in an ISE-SAR if there are "articulable facts or circumstances" that the behavior is "reasonably indicative of pre-operational planning associated with terrorism." ER541. In these cases, again,

further individualized analysis is necessary.[8] This repeated consideration of "the individual facts in the various cases that arise" underscores that the functional standard is a general statement of policy, rather than a legislative rule. *Ryder Truck Lines*, 716 F.2d at 1377.

Rather than "narrow [the] field of vision" available to an analyst (Opening Br. 33 (quoting *Pickus v. U.S. Board of Parole*, 507 F.2d 1107, 1113 (D.C. Cir. 1974))), the functional standard repeatedly encourages analysts to make individualized determinations, using their own judgment, based on "all available knowledge." ER514. Plaintiffs compare the functional standard to legislative rules that "conclusively dispos[e] of certain issues," (Opening Br. 34), but those comparisons are off the mark. *Batterton v. Marshall*, for instance, concerned the Department of Labor's formula for calculating a state's unemployment rate, which directly affected millions of dollars in federal aid to the state. 648 F.2d 694, 697-99 & nn.12, 14 (D.C. Cir. 1980). The agency's formula did not allow for discretion and was promulgated under the agency's authority to "prescribe rules with the force of law concerning" unemployment statistics. *Id.* at 705-07. Likewise, in *McLouth Steel Products Corp. v. Thomas*, the EPA used a scientific model to predict whether a polluter's hazardous materials would leach into groundwater. 838 F.2d 1317, 1319 (D.C. Cir. 1988).

[8] If an analyst were to review a SAR that did not involve one of these sixteen categories of behavior but nevertheless had a direct connection to terrorism, the functional standard states that such a SAR should be sent to the FBI, which can then take further investigative steps as appropriate. ER513-14.

Unless the model gave the polluter a favorable prediction, the polluter would be subject to Subtitle C of the Resource Conservation and Recovery Act, *id.* at 1318-19, and EPA's "stringent regulation[s]" governing hazardous materials under that part of the statute, *Environmental Def. Fund v. EPA*, 852 F.2d 1309, 1311 (D.C. Cir. 1988). None of these agency actions allowed for individualized discretion, and each imposed substantial legal consequences on the regulated party. By contrast, the functional standard repeatedly emphasizes the role of discretion and professional judgment, and imposes no legal consequences on any NSI participant.

Plaintiffs argue that the functional standard constitutes a legislative rule because it uses mandatory language such as "will" and "must." Opening Br. 36-37. But an agency's action does not become a legislative rule simply because it uses particular words. *Clarian Health West, LLC v. Hargan*, 878 F.3d 346, 355, 357-58 (D.C. Cir. 2017) (rejecting argument that agency manual was a legislative rule because it used language such as "will" and "shall"). Rather, the Court examines whether the action imposes right or obligations, or whether it has a "binding effect," *id.* at 357-58, and the D.C. Circuit has noted that the most important factor is "the actual legal effect (or lack thereof) of the agency action in question." *National Mining Ass'n v. McCarthy*, 758 F.3d 243, 252 (D.C. Cir. 2014); *see also Weight Watchers Int'l, Inc. v. FTC*, 47 F.3d 990, 991 n.2 (9th Cir. 1995) (similar, citing the discussion of "legal effect" in *American Mining Cong. v. Mine Safety & Health Admin.*, 995 F.2d 1106, 1112 (D.C. Cir. 1993)).

Plaintiffs also downplay the fact that an agency faces no legal sanctions for disregarding the functional standard. Plaintiffs argue that the lack of legal sanctions does not matter here, relying on *Community Nutrition Institute v. Young*, 818 F.2d 943 (D.C. Cir. 1987), and *Chamber of Commerce v. U.S. Department of Labor*, 174 F.3d 206 (D.C. Cir. 1999). But those cases both involved changes to the legal regime that subjected regulated entities to enforcement proceedings or onerous inspections. In *Community Nutrition*, the Food and Drug Administration published a formal notice in the Federal Register that any food exceeding a certain level of alfatoxin would be considered adulterated, subject to enforcement proceedings and condemnation. 818 F.2d at 947-48. The D.C. Circuit held this to be a legislative rule with legal effect, both because foods exceeding the limit could be subject to condemnation and because foods under the limit were given safe harbor from enforcement proceedings. *Id.* And in *Chamber of Commerce*, an agency required that "each employer in selected industries will be inspected unless it adopts a comprehensive safety and health program." 174 F.3d at 208. These inspections could "be quite as onerous for an employer as paying a fine," and the agency's action was "the practical equivalent of a rule that obliges an employer to comply or to suffer the consequences." *Id.* at 209-10. No such onerous consequences arise here. *See also id.* at 213 (the agency left "no room for discretionary choices by inspectors in the field").

As explained, the functional standard has significant practical benefits and uses for participating agencies, but it lacks legal effect or any enforcement mechanisms.

While agencies "should implement auditing and accountability measures" to ensure that they are protecting "privacy, civil rights, and civil liberties," there are no legal consequences for submitting reports through the NSI SDR that fail to satisfy the reasonably indicative standard. ER515. Of course, if a fusion center analyst determines that information in a SAR does not satisfy the reasonably indicative standard, that report "will not be accessible" through the NSI SDR. ER514. But that is because it is assumed that the analyst will not share the report through the NSI SDR based on that determination; if the analyst does so, however, there are no legal consequences. Conversely, if the analyst determines that a report qualifies as an ISE-SAR because it has a potential nexus to terrorism, but nevertheless decides *not* to share the report, there are no adverse legal consequences—the practical consequences of such a choice are obvious.

The sole incentive for complying with the functional standard is practical—federal, state, local, tribal, and territorial agencies are working together for a common purpose of identifying, disrupting, and preventing terrorist attacks before they occur. The functional standard was collaboratively developed to provide those governments with the best chance possible to achieve that goal, and deviating from the functional standard lessens those governments' ability to have high quality information about potential terrorist threats available. While the functional standard does not bind participating agencies or cause the federal government to impose legal consequences on them, it is nevertheless a critically important standard designed to ensure that there

are no "missed opportunities" to take action against a potential terrorist attack. *The 9/11 Commission Report* 353.[9]

B. The Record Demonstrates That Any Error Was Harmless

Even if the functional standard were a legislative rule, the administrative record in this case demonstrates that the failure to submit the functional standard for notice and comment was harmless. 5 U.S.C. § 706 (court shall take "due account * * * of the rule of prejudicial error"); *Shinseki v. Sanders*, 556 U.S. 396, 406-07 (2009) (explaining that this is a harmless error standard). An agency's failure to provide notice and comment "is harmless only where the agency's mistake clearly had no bearing on the procedure used or the substance of decision reached." *Cal-Almond, Inc. v. USDA*, 14 F.3d 429, 442 (9th Cir. 1993) (quotation marks omitted). The burden is on the plaintiff to demonstrate harmful error. *Northwest Res. Info. Ctr., Inc. v. Northwest Power & Conservation Council*, 730 F.3d 1008, 1020 (9th Cir. 2013).

Plaintiffs complain that the functional standard inappropriately permits agencies to share SARs based on a "reasonably indicative" standard rather than a

[9] Plaintiffs assert that sharing SARs related to potential terrorist threats is not effective. Opening Br. 2, 19. But there is no support for that proposition. Plaintiffs cite a document compiling "Advocate Websites for Concerns and Issues on ISE-related Activities." SER252-58; *see* ER306-09. That document summarized a Congressional Research Service report that recommended creating metrics to determine which ISE-SARs "are meaningful intelligence 'dots,' or whether the right 'dots' are being connected as a result of the program." SER257. Because these metrics analyzing the value of individual ISE-SARs did not yet exist, the Department of Homeland Security could not conduct an empirical analysis comparing the value of ISE-SARs to some other data set. *Id.*

"reasonable suspicion" standard, and inappropriately considers some categories of non-criminal conduct as potentially suspicious. Opening Br. 1-2, 15-16, 33, 51-57. This was also the only alleged harm that plaintiffs identified to the district court. SER5-6. But the functional standard's "reasonably indicative" standard came nearly word-for-word from language proposed by the ACLU. And the functional standard takes pains to explain that potentially non-criminal conduct is not categorically suspicious, and that analysts and law enforcement officers should not deem innocent and constitutionally protected conduct and status as suspicious absent an articulable reason for suspicion. These cautionary instructions were based largely on concerns expressed by the ACLU and other privacy and civil-liberties organizations.

1. The functional standard defines suspicious activity as "[o]bserved behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity." ER504. That definition comes straight from the ACLU, which suggested the definition of "behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." SER346. The government was thus informed of the concerns about its original "may be indicative" standard in Functional Standard 1.0, and it adopted nearly verbatim the heightened standard proposed by the ACLU. *Id.*

Plaintiffs allege that they would have sought to comment that the functional standard should adopt a "reasonable suspicion" standard. ER23 (Gill Decl. ¶ 22); ER91 (Conklin Decl. ¶ 14); ER96 (Ibrahim Decl. ¶ 9); ER109 (Razak Decl. ¶ 24);

ER151 (Prigoff Decl. ¶ 27). But other civil-liberties advocates raised this point and specifically mentioned 28 C.F.R. Part 23. SER367. (The merits of whether 28 C.F.R. Part 23 applies to ISE-SARs are discussed *infra*, pp. 40-46). The government was apprised of this concern through the informal comments it received, and adopted the ACLU's proposed standard. *See* ACLU, *Intelligence Community Raises Its Standards For Information Collection: Collaborative Effort Addresses Privacy and Civil Liberties Concerns*, https://www.aclu.org/print/node/14071 (Functional Standard 1.5, which adopts the reasonably indicative standard, "give[s] law enforcement the authority it needs without sacrificing the rights of those it seeks to protect").

2. Plaintiffs also allege that they would have provided comments presenting their personal stories, which would be "concrete illustration[s] of how the Functional Standard encourages religious profiling." SER5. But in developing the functional standard, the government proactively requested "specific examples of incidents where suspicious activity collection resulted in over-zealous police behavior," so it could appropriately modify the functional standard to address this. SER343. And the ACLU responded to this request, providing the government with specific examples of instances where citizens felt they had been harassed by law enforcement officers based on their religious beliefs, political views, or constitutionally protected activity. SER344-45. Plaintiffs' additional personal anecdotes would not have provided any qualitatively different information, nor would they have resulted in a different standard.

Furthermore, the ACLU had provided comments that the original functional standard was problematic because it did not distinguish "innocuous, innocent, and First Amendment-protected activity" from "obviously criminal activity." SER346. Without distinguishing between these kinds of behavior and providing appropriate cautionary instructions, the ACLU expressed concern that the functional standard may encourage "racial and/or religious profiling as officers use their own discretion to decide what 'photography' might suggest possible terrorist activity." SER347. Accordingly, the ACLU recommended listing the "obviously criminal activity first," and the non-criminal activity "second, with more detailed descriptions that emphasize the necessity for facts raising a suspicion of criminality before reporting is appropriate." *Id.* Additionally, the ACLU recommended that the functional standard should clarify that "race and religion should not be considered as factors that create reasonable suspicion (except if used as specific suspect descriptions)." *Id.* All of these suggestions were incorporated into the functional standard. ER510-11, 513, 541-51.

Assuming arguendo that the functional standard should have been submitted for notice and comment, the plaintiffs do not identify any way in which they have been harmed. Their alleged comments covered issues "that had been extensively commented on" by the ACLU and other civil-liberties groups during the collaborative process of developing the functional standard. *Safari Aviation, Inc. v. Garvey*, 300 F.3d 1144, 1152 (9th Cir. 2002). Although it certainly will not always be the case that a

failure to follow the notice-and-comment procedures in 5 U.S.C. § 553 will be harmless, this is the unique case where the record demonstrates no prejudicial error. *See City of Los Angeles v. U.S. Dep't of Commerce*, 307 F.3d 859, 877 (9th Cir. 2002) ("[W]e know that the result would have been exactly the same."). [10]

III. THE FUNCTIONAL STANDARD DOES NOT CONFLICT WITH 28 C.F.R. PART 23, BECAUSE PART 23 DOES NOT APPLY TO SARS CONCERNING POTENTIAL TERRORIST THREATS

Plaintiffs argue that the functional standard is arbitrary and capricious because it applies a "reasonably indicative" standard for sharing ISE-SARs through the NSI, rather than the "reasonable suspicion" standard set forth in 28 C.F.R. § 23.20(a) for sharing criminal intelligence information. The district court noted that plaintiffs' argument "presupposes that SARs are 'criminal intelligence' [information] governed under Part 23." ER9. The functional standard, however, was "developed to address

[10] If the Court were to disagree and hold that the functional standard must be promulgated through notice and comment under 5 U.S.C. § 553, the current functional standard should be left in place while that process plays out. "[W]hen equity demands, the regulation can be left in place while the agency follows the necessary procedures" to correct its action. *California Communities Against Toxics v. EPA*, 688 F.3d 989, 992 (9th Cir. 2012). The equities here strongly counsel against vacating the functional standard—vacatur would create substantial uncertainty about the ability of national security and law enforcement agencies to share essential information about potential terrorist threats. This Court and others have declined to vacate agency rules when vacatur would have imposed substantial threats to the public interest. *See Electronic Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 8 (D.C. Cir. 2011) (declining to vacate rule when vacatur would "severely disrupt an essential security operation"); *California Communities Against Toxics*, 688 F.3d at 992-94 (collecting cases and declining to vacate rule when vacatur would have deprived many people of electricity).

data collection and dissemination issues not already within the scope of Part 23," and the government's decision to adopt a standard different from 28 C.F.R. § 23.20(a) is neither arbitrary nor capricious. ER9.

The regulations in Part 23 govern the investigation and "exchange of intelligence data" of "ongoing networks of criminal activity" that participate in crimes such as "loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials." 28 C.F.R. § 23.2. Part 23 was designed to regulate the dissemination of information "concerning an individual" in such cases when "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). These regulations were first promulgated in 1980 by the Department of Justice, 45 Fed. Reg. 61,612 (Sept. 17, 1980), and revised in 1993, 58 Fed. Reg. 48,448 (Sept. 16, 1993). As shown below, the Department has consistently explained that Part 23 does not generally apply to suspicious activity reports that have a potential nexus to terrorism and are shared through the NSI SDR.

This Court has consistently recognized that federal agencies are "entitled to deference to their interpretation of their own regulations," *Native Ecosystems Council v. U.S. Forest Serv.*, 418 F.3d 953, 960 (9th Cir. 2005), because in interpreting an administrative regulation, the Court "must necessarily look to the administrative construction of the regulation," *Bowles v. Seminole Rock & Sand Co.*, 325 U.S. 410, 414

(1945). Accordingly, the Court's "task is not to decide which among several competing interpretations best serves the regulatory purpose," but whether the agency's interpretation is "plainly erroneous or inconsistent with the regulation." *Thomas Jefferson Univ. v. Shalala*, 512 U.S. 504, 512 (1994). So long as it satisfies that standard, the agency's interpretation is controlling. *Auer v. Robbins*, 519 U.S. 452, 461 (1997). This deference is warranted when the Department of Justice files a brief in the court of appeals that "includes an interpretation of the relevant * * * regulations" promulgated by the Department. *K.M. ex rel. Bright v. Tustin Unified Sch. Dist.*, 725 F.3d 1088, 1092 (9th Cir. 2013).

As recounted *supra*, pp. 14-18, the Department of Justice and other governmental actors consistently understood that Part 23 did not generally apply to ISE-SARs shared through the NSI SDR, but could apply in certain circumstances. As early as 2007, the Department explained that SARs were "[t]ips and leads data [that] are not criminal intelligence [information] as defined by 28 Code of Federal Regulation (CFR) Part 23." SER351, 356. That is because Part 23 governs information about a specific "individual who or organization which is reasonably suspected of involvement in criminal activity," such as loan sharking, drug trafficking, gambling, extortion, and the like. 28 C.F.R. §§ 23.2, 23.3(b)(3)(i). By contrast, information about potential terrorist threats are not necessarily tied to specific individuals or organizations, nor will individual reports consistently rise to the level of reasonable suspicion. One of the critical lessons of the September 11th attacks "is

that individual 'dots' of information may not paint a picture until a later-acquired piece of information ties them together." SER326. And while it "may be difficult to determine whether a single incident * * * has a nexus to terrorism," that connection can become clear once "many outwardly unrelated tips, leads, and suspicious incidents" are "analyzed, shared, and combined with other seemingly unrelated information at the local, state, regional, and federal levels." SER354.

This reasoning is consistent with the federal courts' understanding of how, in the national security context, individual pieces of information may not be significant in and of themselves, but when they are collected together, they can reveal vitally important information. "Minor details of intelligence information may reveal more information than their apparent insignificance suggests because, much like a piece of a jigsaw puzzle, [every detail] may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself." *Hamdan v. U.S. Dep't of Justice*, 797 F.3d 759, 775 (9th Cir. 2015) (quoting *Larson v. Department of State*, 565 F.3d 857, 864 (D.C. Cir. 2009)). "Bits and pieces of information that may appear innocuous in isolation" may be collected to form a "bigger picture" in a terrorism investigation. *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 706 (6th Cir. 2002). Like the "construction of a mosaic," an individual report of suspicious activity may not appear "of obvious importance until pieced together with other pieces of information." *Id.*

See also ACLU v. DOJ, 681 F.3d 61, 71 (2d. Cir. 2012) (similar).[11] As the Supreme Court has explained, a trivial piece of information to an uninformed observer "may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context." *CIA v. Sims*, 471 U.S. 159, 178 (1985).

The regulations of Part 23 govern the dissemination of criminal intelligence information tied to specific individuals and organizations reasonably suspected of engaging in criminal activity—they do not speak to whether government agencies may share SARs that, while not rising to the level of reasonable suspicion of a particular crime, nevertheless may play an important role in detecting a potential terrorist threat before it materializes. As an illustrative example, a SAR might report that a person enters a shipping port, refuses to identify himself, asks to enter a secured area, and inquires about the presence of military personnel. ER547. After he notices that security officers have been contacted, the person runs away and leaves the scene in a car with out-of-state plates. *Id.* Regardless of whether such a report would provide "reasonable suspicion" that a particular crime has been committed, it ought to be

[11] *Cf. Bassiouni v. CIA*, 392 F.3d 244, 246 (7th Cir. 2004) ("When a pattern of responses itself reveals classified information, the only way to keep secrets is to maintain silence uniformly."); *American Friends Serv. Comm. v. Department of Defense*, 831 F.2d 441, 444-45 (3d Cir. 1987) ("[I]nformation harmless in itself might be harmful when disclosed in context.").

shared through the NSI SDR, and nothing within Part 23 prohibits sharing this kind of information.

In some circumstances, however, an ISE-SAR could contain information that rises to the level of reasonable suspicion that a particular person or organization is involved in a definable criminal activity or enterprise. When that happens, the agency submitting the ISE-SAR to the NSI SDR (or its forerunner, ISE-SAR Shared Spaces) "may also make a submission to a criminal intelligence information database or system" consistent with Part 23. SER69; *see also* SER68 (explaining that ISE-SAR Shared Spaces "is not a criminal intelligence system or database" under Part 23).

During the development of the functional standard, the Department of Justice and the Program Manager expressed their views that Part 23 does not generally apply to ISE-SARs, but might apply to information contained within an ISE-SAR based on the particular circumstances. In 2008, the Program Manager, in consultation with the Department of Justice, explained that "'[r]easonable suspicion' is not a separate requirement of the ISE-Functional Standard" because ISE-SARs are "considered fact-based information rather than criminal intelligence" information. ER440. But when the information in an ISE-SAR "also meets 28 CFR Part 23 criteria, it may be submitted to a criminal intelligence information database * * * under 28 CFR Part 23." *Id.* The Department also issued a report illustrating that terrorism-related SARs should be shared through ISE Shared Spaces, while information in a SAR that establishes reasonable suspicion should be submitted to and disseminated through a

criminal intelligence database under Part 23. ER289. In sharing collaborative draft reports with the ACLU, the Program Manager reiterated the view that the "reasonably indicative" standard was different from, but could interact with, "other requirements such as 28 CFR Part 23." SER382.

The functional standard incorporated these previously expressed views, stating that an ISE-SAR shared through the NSI SDR "may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23." ER555. The executive summary accompanying the functional standard stated that ISE-SARs "represent[] information about suspicious behavior" related to terrorism, which is different from criminal intelligence information that focuses instead on "the specific criminal subject(s), the criminal activity in which they are engaged, and the evaluation of facts to determine that the reasonable suspicion standard has been met." ER500.

The Department's consistent interpretation of 28 C.F.R. Part 23—and its interaction with the functional standard—is entitled to deference. The Department's interpretation is not "plainly erroneous or inconsistent with the regulation," and it is consistent with the government's longstanding view held during the development of the functional standard, prior to this litigation. *Decker v. Northwest Envtl. Def. Ctr.*, 568 U.S. 597, 613-14 (2013). Plaintiffs' assertions that the government failed to address Part 23 at all (Opening Br. 45-51), or that its current interpretation is a *post hoc*

rationalization (Opening Br. 57-61), are mistaken and contradicted by the record as described above.

CONCLUSION

The district court's judgment should be affirmed.

Respectfully submitted.

CHAD A. READLER
Acting Assistant Attorney General

ALEX G. TSE
Acting United States Attorney

H. THOMAS BYRON III
(202) 616-5367
/s/ Daniel Aguilar
DANIEL AGUILAR
(202) 514-5432
Attorneys, Appellate Staff
Civil Division, Room 7266
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

STATEMENT OF RELATED CASES

We are not aware of any related cases before this Court.

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the requirements of Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in 14-point Garamond, a proportionally spaced font. I further certify that this brief complies with the type-volume limitation of Circuit Rule 32-1(a) because it contains 11,136 words, excluding the parts of the brief exempted under Rule 32(f), according to the count of Microsoft Word.

/s/ Daniel Aguilar
Daniel Aguilar

CERTIFICATE OF SERVICE

I certify that on February 16, 2018, I caused the foregoing brief to be electronically filed with the United States Court of Appeals for the Ninth Circuit via the CM/ECF system, which will serve counsel of record for all parties.

/s/ Daniel Aguilar
Daniel Aguilar

ADDENDUM

ADDENDUM TABLE OF CONTENTS

Page

5 U.S.C. § 553. Rule making

(a) This section applies, according to the provisions thereof, except to the extent that there is involved—

(1) a military or foreign affairs function of the United States; or

(2) a matter relating to agency management or personnel or to public property, loans, grants, benefits, or contracts.

(b) General notice of proposed rule making shall be published in the Federal Register, unless persons subject thereto are named and either personally served or otherwise have actual notice thereof in accordance with law. The notice shall include—

(1) a statement of the time, place, and nature of public rule making proceedings;

(2) reference to the legal authority under which the rule is proposed; and

(3) either the terms or substance of the proposed rule or a description of the subjects and issues involved.

Except when notice or hearing is required by statute, this subsection does not apply—

(A) to interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice; or

(B) when the agency for good cause finds (and incorporates the finding and a brief statement of reasons therefor in the rules issued) that notice and public procedure thereon are impracticable, unnecessary, or contrary to the public interest.

(c) After notice required by this section, the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation. After consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose. When rules are required by statute to be made on the record after opportunity for an agency hearing, sections 556 and 557 of this title apply instead of this subsection.

(d) The required publication or service of a substantive rule shall be made not less than 30 days before its effective date, except—

(1) a substantive rule which grants or recognizes an exemption or relieves a restriction;

(2) interpretative rules and statements of policy; or

(3) as otherwise provided by the agency for good cause found and published with the rule.

(e) Each agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule.

5 U.S.C. § 704. Actions reviewable

Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review. A preliminary, procedural, or intermediate agency action or ruling not directly reviewable is subject to review on the review of the final agency action. Except as otherwise expressly required by statute, agency action otherwise final is final for the purposes of this section whether or not there has been presented or determined an application for a declaratory order, for any form of reconsideration, or, unless the agency otherwise requires by rule and provides that the action meanwhile is inoperative, for an appeal to superior agency authority.

5 U.S.C. § 706. Scope of review

To the extent necessary to decision and when presented, the reviewing court shall decide all relevant questions of law, interpret constitutional and statutory provisions, and determine the meaning or applicability of the terms of an agency action. The reviewing court shall—

(1) compel agency action unlawfully withheld or unreasonably delayed; and

(2) hold unlawful and set aside agency action, findings, and conclusions found to be—

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

(B) contrary to constitutional right, power, privilege, or immunity;

(C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right;

(D) without observance of procedure required by law;

(E) unsupported by substantial evidence in a case subject to sections 556 and 557 of this title or otherwise reviewed on the record of an agency hearing provided by statute; or

(F) unwarranted by the facts to the extent that the facts are subject to trial de novo by the reviewing court.

In making the foregoing determinations, the court shall review the whole record or those parts of it cited by a party, and due account shall be taken of the rule of prejudicial error.

6 U.S.C. § 485. Informating sharing

* * *

(b) Information sharing environment

(1) Establishment

The President shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) Attributes

The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE 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. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

> (A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;
>
> (B) ensures direct and continuous online electronic access to information;
>
> (C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;
>
> (D) builds upon existing systems capabilities currently in use across the Government;
>
> (E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
>
> (F) facilitates the sharing of information at and across all levels of security;
>
> (G) provides directory services, or the functional equivalent, for locating people and information;
>
> (H) incorporates protections for individuals' privacy and civil liberties;
>
> (I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;
>
> (J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;
>
> (K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;

(L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;

(M) permits analysts to collaborate both independently and in a group (commonly known as "collective and noncollective collaboration"), and across multiple levels of national security information and controlled unclassified information;

(N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and

(O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

* * *

(f) Program manager

(1) Designation

Not later than 120 days after December 17, 2004, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. The individual designated as the program manager shall serve as program manager until removed from service or replaced by the President (at the President's sole discretion). The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

(2) Duties and responsibilities

(A) In general

The program manager shall, in consultation with the Information Sharing Council—

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;

(iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;

(iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and

(v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) Content of policies, procedures, guidelines, rules, and standards

The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

28 C.F.R. Part 23

28 C.F.R. § 23.1. Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended (Pub.L. 90–351, as amended by Pub.L. 91–644, Pub.L. 93–83, Pub.L. 93–415, Pub.L. 94–430, Pub.L. 94–503, Pub.L. 95–115, Pub.L. 96–157, Pub.L. 98–473, Pub.L. 99–570, Pub.L. 100–690, and Pub.L. 101–647), are utilized in conformance with the privacy and constitutional rights of individuals.

28 C.F.R. § 23.2. Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

28 C.F.R. § 23.3. Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended (Pub.L. 90–351, as amended by Pub.L. 91–644, Pub.L. 93–83, Pub.L. 93–415, Pub.L. 94–430, Pub.L. 94–503, Pub.L. 95–115, Pub.L. 96–157, Pub.L. 98–473, Pub.L. 99–570, Pub.L. 100–690, and Pub.L. 101–647).

(b) As used in these policies:

(1) *Criminal Intelligence System* or *Intelligence System* means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information;

(2) *Interjurisdictional Intelligence System* means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions;

(3) *Criminal Intelligence Information* means data which has been evaluated to determine that it:

(i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and

(ii) Meets criminal intelligence system submission criteria;

(4) *Participating Agency* means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system;

(5) *Intelligence Project* or *Project* means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and

(6) *Validation of Information* means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

28 C.F.R. § 23.20. Operating principles.

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

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) *Reasonable Suspicion* or *g* is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

> (1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and
>
> (2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(ii) [Reserved]

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99–508, 18 U.S.C. 2510–2520, 2701–2709 and 3121–3125, or any applicable State statute related to wiretapping and surveillance.

(*l*) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

28 C.F.R. § 23.30. Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and

supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) (1) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(i) Assume official responsibility and accountability for actions taken in the name of the joint entity, and

(ii) Certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

(2) The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

28 C.F.R. § 23.40. Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR part 23 Criminal Intelligence Systems Policies.