IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

AL-HARAMAIN ISLAMIC)
FOUNDATION, INC., et al.,)
Plaintiffs/Appellees,)
v.) No. 09-15266
BARACK H. OBAMA, President of the)
United States, et al.,)
)
Defendants/Appellants.)

REPLY IN SUPPORT OF EMERGENCY MOTION FOR STAY PENDING APPEAL AND OPPOSITION TO MOTION TO DISMISS

MICHAEL F. HERTZ Acting Assistant Attorney General

DOUGLAS N. LETTER THOMAS M. BONDY H. THOMAS BYRON III Attorneys, Appellate Staff Civil Division, Room 7513 Department of Justice 950 Pennsylvania Ave., N.W. Washington, D.C. 20530-0001 202-514-3602

INTRODUCTION AND SUMMARY

A stay here is plainly warranted. The district court has held that Congress, in enacting FISA, abrogated the state secrets privilege in the electronic surveillance context. On that basis, the district court has provided for plaintiffs' counsel to obtain top secret/sensitive compartmented information security clearances, and has made clear that it will provide those counsel with access to classified information that this Court has held is encompassed by the state secrets privilege. A stay is called for to allow this Court to conduct appellate review in an orderly fashion without the occurrence of irreparable harm to the public interest in the protection of national security information. It is settled that where a district court order threatens to disclose protected information, a stay pending appeal is warranted to protect the authority of the appellate court to exercise meaningful review. The status quo should be preserved here so that no improper disclosures take place while this Court is considering the underlying issues on their merits.

There is no question that irreparable harm is likely to occur absent a stay. Plaintiffs note that the district court has not set out in full detail how it intends to proceed. The district court has made clear, however, that it will provide plaintiffs' counsel with access to classified information over the objections of the Executive. That access, once granted, cannot be undone. Not only would disclosure of information to plaintiffs' counsel be wholly improper because the NSA Director has determined that counsel have no valid "need to know," but, in addition, even issuance of sealed orders in this case risks revealing classified information.

The Government has established a substantial likelihood of success on the merits. Plaintiffs argue that the district court properly held the state secrets privilege displaced by FISA, but that statute by its terms nowhere refers to the privilege. Where, as here, the question is whether a statute was intended to abrogate a privilege deeply rooted in the Constitution and the common law, a clear and explicit statement by Congress in the legislation is required, and Congress will not be presumed to have effected such abrogation implicitly. No such clear statement is present here, and, indeed, no other court has ever held that FISA preempts the state secrets privilege.

The district court's treatment of classified information is also legally incorrect. The NSA Director has determined that plaintiffs' counsel have no "need to know" the classified information at issue. Plaintiffs assert that the district court has the authority to make its own need-to-know determination. But the Supreme Court has made clear that the grant of a security clearance is committed by law to the appropriate agency of the Executive Branch, and flows from a constitutional investment of power in the President. <u>Department of the Navy v. Egan</u>, 484 U.S. 518 (1988).

Plaintiffs' motion to dismiss this appeal should be denied. The district court's failure to diagram exactly what its next steps will be does not preclude appellate review. As noted, the district court has made clear that it intends to provide

- 2 -

plaintiffs' counsel with access to classified information that this Court has held lies within the scope of the state secrets privilege. The Government is not required to wait for irreparable harm to occur before seeking relief from this Court.

The district court's order is immediately reviewable, either as a collateral order or an injunction. Under plaintiffs' interpretation of the January 5 order, the district court will itself determine that plaintiffs' counsel have a need to know classified information, contravening the Executive Branch's contrary determination. Such an assertion of authority by the district court is a final determination of a collateral matter, and jurisdiction is thus proper under 28 U.S.C. § 1291. Alternatively, the district court's order can be read to compel the Government to grant a need-to-know determination, despite the contrary dictates of governing law and the exercise of expert judgment by responsible Executive officials. Under that reading, the order is appealable as an injunction. Either way, immediate review is available, and the Government's appeal is properly before this Court.

ARGUMENT

I. This Court Should Stay Proceedings That Will Lead To Disclosure Of Classified Information.

A. Balance Of Harms And The Public Interest.

Our motion showed that a stay is warranted because the district court's order threatens to disclose classified national security information over the objection of the Executive and in the face of a determination by the responsible agency that plaintiffs' attorneys do not have a need to know the classified information. As we explained, especially given the sensitivity of the information at issue, no reason exists to allow the status quo to be irrevocably altered during the pendency of our appeal. The appeal manifestly raises serious questions on the merits, and disclosure of classified information while the appeal is pending would cause irreparable injury. It is well-settled that where a district court order threatens to disclose otherwise protected information, a stay pending appeal is necessary to protect both the information and the authority of the appellate court to exercise meaningful review. <u>See, e.g.</u>, <u>Providence Journal Co. v. FBI</u>, 595 F.2d 889, 890 (1st Cir. 1979).

That basic principle – that the status quo should be preserved pending appeal so that no improper disclosures take place while this Court is considering the underlying issues on their merits – underlies our stay request. Plaintiffs do not come to grips with this bedrock point.

Instead, plaintiffs' main contention that no harm would result absent a stay is really a deficient merits argument. Plaintiffs note that this Court remanded the case for the district court to consider their allegation that FISA preempts the state secrets privilege. According to plaintiffs, "[i]mplicit in that decision is the assumption that section 1806(f) *can* be employed effectively to protect national security in this case – otherwise, the remand would have been pointless." Opp. 15 (emphasis in original).

Plaintiffs' assertion is untenable. This Court remanded the matter for the district court to consider plaintiffs' FISA preemption argument in the first instance. This Court did not pass upon that argument in any respect, and neither "implicit[ly]" (Opp. 15) nor explicitly suggested that FISA procedures could satisfy the national security concerns underlying the state secrets privilege.

Plaintiffs are similarly mistaken in urging that the Government's stay request "collapses * * * if FISA *preempts* the state secrets privilege. The district court has ruled that FISA *does* preempt" the privilege. Opp. 2 (emphasis in original). The whole point of our appeal is that, in the Government's view, the district court *legally erred* in coming to that conclusion, and, likewise, the point of our stay motion is that the status quo should be preserved while this Court has an opportunity, in an orderly fashion, to pass upon that novel legal ruling.

Indeed, plaintiffs ultimately concede the point: They recognize that "[i]f the state secrets privilege were to apply to this case, this Court has indicated that the district court would not be permitted to disentangle portions of the Sealed Document * * * and allow plaintiffs to use those portions to demonstrate standing, but would have to exclude the Sealed Document entirely." Opp. 13. That statement is correct, and underscores why a stay is needed. The district court is poised to determine "whether the Sealed Document establishes that plaintiffs were subject to electronic surveillance not authorized by FISA." 1/5/09 Order at 23. The district court's

inquiry regarding the Sealed Document, along with further orders and proceedings flowing from that inquiry, is flatly barred by this Court's 2007 decision, "unless FISA preempts the state secrets privilege." 507 F.3d at 1205. Before the district court embarks upon such a drastic and, in our view, mistaken, course, a stay should enter to safeguard against any improper disclosures pending appellate review.

Plaintiffs mistakenly suggest that there is no danger that classified information will be disclosed. Opp. 11-12. The district court has expressly decided that the state secrets privilege does not apply. It has "provided for plaintiffs' counsel to obtain top secret/sensitive compartmented information security clearances." 2/13/09 Order at 2. And, as the court has plainly stated, it intends "that 'both parties have access to the material upon which the court makes a decision." <u>Id</u>. at 3. There is thus no question that the court will share at least some classified information with plaintiffs' counsel.

The risk of harm here is not limited to overt public disclosures. <u>See</u> Opp. 14. Disclosure of information to plaintiffs' counsel would itself be improper because counsel have no "need to know," and, in addition, even issuance of sealed orders in the context of this case risks revealing classified information. <u>See</u> Stay Motion at 12-13. Indeed, courts have cautioned against the risk of "further disclosure – inadvertent, mistaken, or even intentional" – as a reason to limit dissemination of national security information. <u>Sterling v. Tenet</u>, 416 F.3d 338, 344 (4th Cir. 2005).

In short, the district court has held that Congress preempted the state secrets

privilege, and, on that basis, has made clear that it intends to effect classified information disclosures that are unauthorized by the Executive Branch. A stay is warranted under these circumstances, so that this Court can consider the merits of the underlying appeal without irreparable harm occurring in the interim.¹/

B. Likelihood Of Success On The Merits.

1. Plaintiffs' opposition to a stay is particularly implausible given the nature of the district court's legal holding that is the focus of the Government's appeal. The district court held that Congress, in enacting FISA, preempted the state secrets privilege. But that statute nowhere references the state secrets privilege. The court's conclusion that a statute that does not mention the state secrets privilege nonetheless vitiates the President's power to invoke it is, at a minimum, open to serious question.

Indeed, while plaintiffs stress the common law heritage of the state secrets privilege, <u>see</u> Opp. 18, they omit that the privilege has constitutional roots, reflecting the Executive's constitutional authority regarding national security. <u>See El-Masri v.</u> <u>United States</u>, 479 F.3d 296, 303-04 (4th Cir. 2007) (citing <u>United States v. Nixon</u>, 418 U.S. 683, 710 (1974)). And, as our stay motion explained, the courts will not read

^{1/} Plaintiffs inaptly repeat their amended complaint's allegations regarding alleged public statements of FBI Deputy Director Pistole. <u>See</u> Opp. 15. As the Government has noted in fuller detail in its district court papers, plaintiffs selectively quote Mr. Pistole out of context, and his actual statements provide no support for plaintiffs' position. <u>See</u> Doc. 49 at 16-17; Doc. 54 at 10.

a statute to interfere with the President's constitutional authority unless Congress has made clear in the statutory text its intent to do so. <u>See Franklin v. Massachusetts</u>, 505 U.S. 788, 801 (1992) ("We would require an express statement by Congress before assuming it intended the President's performance of his statutory duties to be reviewed for abuse of discretion."); <u>Armstrong v. Bush</u>, 924 F.2d 282, 289 (D.C. Cir. 1991). As noted, FISA's text contains no allusion to the state secrets privilege, and the clear statement prerequisite is thus manifestly not satisfied.

The same analysis applies even if the state secrets privilege is viewed only in terms of its common law pedigree. Again, a privilege with deep common law roots "ought not to be deemed repealed, unless the language of a statute be clear and explicit for this purpose." <u>Norfolk Redev. & Hous. Auth. v. Chesapeake & Potomac Tel. Co.</u>, 464 U.S. 30, 35 (1983); <u>Kasza v. Browner</u>, 133 F.3d 1159, 1167-68 (9th Cir. 1998). No such "clear and explicit" expression of Congressional intent exists here, and plaintiffs do not seriously argue otherwise.

Arguing in favor of <u>implicit</u> preemption, plaintiffs assert that FISA would in certain respects be rendered meaningless if it did not abrogate the state secrets privilege. Opp. 20. Had Congress meant to infringe upon the state secrets privilege through FISA, it would have said so explicitly, giving the President the ability to fully consider the bill and whether to exercise his veto power. In any event, Section 1806(f) is not meaningless; it provides aggrieved persons with a shield against the Government's affirmative use of information obtained from disclosed electronic surveillance. The district court's holding that FISA additionally provides a vehicle for persons to discover whether they have been subjected to NSA surveillance, based on their own <u>allegations</u> of surveillance – notwithstanding the state secrets privilege and the Executive's constitutional authority to control access to classified information – is without basis in FISA's text and history.

Indeed, in disparaging the Government's likelihood of success on appeal, plaintiffs overlook the unprecedented nature of the district court's determination. No other court has ever held that FISA displaces the state secrets privilege. Even apart from its evident significance, the novel quality of the legal ruling at issue here calls for a stay while this Court undertakes appellate review.

2. The district court's treatment of classified information is also legally incorrect. The governing Executive Order establishes that, before classified information can be disclosed to an individual, three independent conditions must be satisfied: First, the relevant Executive agency must determine that the recipient is trustworthy. Second, the recipient must sign an approved non-disclosure agreement. And, third, the recipient must have a "need to know" the classified information. <u>See</u> Exec. Order 12958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Exec. Order 13292, 68 Fed. Reg. 15315, 15324 (Mar. 25, 2003). The need-to-know standard is satisfied only if the responsible Executive agency determines that the "prospective

recipient requires access to specific classified information to perform or assist in a lawful and authorized governmental function." 68 Fed. Reg. 15322.

Here, the responsible Executive official – the NSA Director – has determined that plaintiffs' counsel <u>do not</u> have a need to know the classified information at issue. <u>See</u> Cerlenko Decl. ¶ 9 (attached). Indeed, "disclosure of this information would cause exceptional harm to national security." <u>Ibid</u>.

Plaintiffs' position is that the district court is invested with authority to make the need-to-know determination, and that the court may thus override the judgment of the responsible intelligence officials in the Executive Branch. Opp. 16. Plaintiffs cite no authority supporting this startling proposition, and we are aware of none.

Plaintiffs' reliance on Executive Order 13292 is misplaced. <u>See</u> Opp. 16. The Executive Order does not make a court an "authorized holder" of classified information. The Executive agency responsible for the information – here, NSA – is the "authorized holder," and nothing in the language of the Executive Order suggests otherwise. <u>See</u> EO 13292, 68 Fed. Reg. 15315.

To the contrary, the Supreme Court has made clear that the grant of a security clearance, and the authority to determine who or how many persons shall have access to classified information, "is committed by law to the appropriate agency of the Executive Branch," and "flows primarily from [a] constitutional investment of power in the President." <u>Department of the Navy v. Egan</u>, 484 U.S. 518, 526-27 (1988).

Indeed, as the Supreme Court has stressed, the authority "to classify and control access to information bearing on national security" is constitutionally vested in the President as head of the Executive Branch and as Commander in Chief. See ibid.^{2/}

Plaintiffs do not cite <u>Egan</u>, but the Supreme Court's holding and rationale there are dispositive. Especially in light of <u>Egan</u>, the district court's analysis, at an absolute minimum, is open to sufficiently serious question so as to warrant a stay.

II. The Government's Appeal Is Properly Before This Court.

Plaintiffs' motion to dismiss the Government's appeal for lack of jurisdiction should be denied. The district court's January 5 order provides for the disclosure of classified information to plaintiffs' counsel over the objection of the Executive. The district court has left no doubt – and plaintiffs do not dispute – that it will disclose classified information to counsel, and it intends to do so under the aegis of FISA Section 1806(f).

Even if the January 5 order leaves some ambiguity concerning exactly how the

 $[\]frac{2}{2}$ Judge Rogers' concurring and dissenting opinion in <u>United States v. Pollard</u>, 416 F.3d 48 (D.C. Cir. 2005), cited by plaintiffs (<u>see</u> Opp. 17), is not to the contrary. The majority there held that the courts had no authority to compel the Executive Branch to disclose classified documents to a prisoner's counsel for purposes of a clemency petition. <u>Id</u>. at 56-57. Judge Rogers agreed that the request for documents should be denied. In her view, the courts possessed jurisdiction to consider the request in light of an agreed-upon protective order giving the district court authority over the documents in conjunction with the underlying criminal proceedings. <u>Id</u>. at 58-59. Nothing in Judge Rogers' analysis suggests that the district court has the authority to override the Executive's need-to-know determination here.

district court intends to override the NSA Director's determination that plaintiffs' counsel do not have a need to know under the governing executive order, the order is still appealable. The court might itself purport to make a contrary need-to-know determination (as plaintiffs urge in their filings below and in their motion to dismiss). Under that reading, the January 5 order is an appealable collateral order under 28 U.S.C. § 1291. Or, the district court may read its January 5 order as compelling the Executive Branch to grant a need-to-know determination as part of the processing of security clearances for plaintiffs' counsel ordered by the court (as the most recent order denying the stay would suggest in its reference to compliance by the Government with the January 5 order's requirements). Such an interpretation demonstrates the injunctive nature of the district court's order, giving this Court jurisdiction under 28 U.S.C. § 1292(a)(1).

Either way, such disclosure is prohibited by governing law, would cause exceptionally grave harm to national security, and would result in irreparable injury. Plaintiffs are wrong to suggest that this Court is powerless in the face of such consequences. The Government need not wait until its secrets are divulged before seeking relief in this Court. Whichever interpretation of the January 5 order governs (and, thus, whichever theory of jurisdiction applies), the Government is entitled to review of the serious constitutional and legal questions posed by the district court's plan before that court finalizes the irreversible step of disclosure.

A. Collateral Order.

The January 5 order is appealable under the collateral-order doctrine, which generally permits an interlocutory appeal where privileged information is ordered to be disclosed. "In order to be reviewable under the collateral order doctrine, a decision must [1] conclusively determine the disputed question, [2] resolve an important issue completely separate from the merits of the action, and [3] be effectively unreviewable on appeal from a final judgment." In re Napster, Inc. Copyright Litigation, 479 F.3d 1078, 1088 (9th Cir. 2007). This Court has "repeatedly held that where * * * a district court holds, following full development of the issues by the parties, that a privilege has been vitiated, its order constitutes a conclusive determination." Ibid. (citing cases). That principle is unsurprising: Where privileged information is subject to disclosure, an immediate appeal is necessary to protect the authority of the appellate court and prevent mootness that could otherwise result from premature disclosure of the privileged information.

The district court has conclusively resolved for purposes of this case the question whether FISA displaces the state secrets privilege, and has invoked that statute in creating an unprecedented mechanism for in camera review, disclosure of classified information to private counsel, and determinations of national security matters whose disclosure would cause exceptionally grave harm to national security. Those steps are significant and separate from the underlying merits of the suit, which

involve whether the Government, through the TSP, violated plaintiffs' rights under the Constitution and FISA's electronic surveillance provisions. The merits question – whether the Government violated FISA or the Constitution – is distinct from the question of whether and how the district court may go about adjudicating such claims and whether the court can disclose classified information to private counsel over the objection of the Executive.

The district court here held that FISA displaces the state secrets privilege, and that due process compels disclosure of privileged and classified information to plaintiffs' counsel. That is a classic example of a collateral order. It conclusively determines the question whether the state secrets privilege applies, and disclosure to plaintiffs' counsel now would cause irreparable harm.

Plaintiffs' reading of the January 5 order is fully consistent with this view. Plaintiffs take the position that the district court can and should unilaterally disclose classified information to plaintiffs' counsel. <u>See</u> Opp. 16-17. The collateral order doctrine thus permits immediate review of an order that would otherwise be unreviewable after further proceedings are complete.^{3/}

 $[\]frac{3}{2}$ It is no answer that "the ruling leaves unsettled, for the time being, the questions of how and to what extent plaintiffs' counsel will be granted access to classified information." Opp. 5. Plaintiffs' counsel seek, and the district court has ruled that it will provide, access to classified information. No matter how that extraordinary action is accomplished, it would cause irreparable harm, and the imminent threat of such disclosure warrants immediate review by this Court.

B. Injunction.

The January 5 order is also appealable as an order granting an injunction. Section 1292(a) permits immediate appeal of "interlocutory orders * * * granting * * * injunctions." 28 U.S.C. § 1292(a)(1). The district court order directed the Government to process security clearances for plaintiffs' counsel. See 1/5/09 Order at 23-24. The Government has conducted the requisite background checks, but has informed the court that counsel are not authorized to receive the classified information at issue here under the governing executive orders, because they do not have a "need to know." Most recently, in denying a stay, the district court directed the Government "to inform the court how it intends to comply with the January 5 order." 2/13/09 Order at 3. The court explained in the same order that the January 5 order "put in place" a "procedure" under which "[t]he court seeks from the government implementation of the steps necessary to afford that both parties have access to the material upon which the court makes a decision." Ibid. (internal quotation marks omitted). The quoted language reflects the court's interpretation of its January 5 order as requiring the Government to grant a need-to-know determination, contrary to the governing executive orders and the judgment of responsible Executive officials. $\frac{4}{}$

⁴/ Plaintiffs thus incorrectly assert that the Government has already fully complied with the injunctive aspects of the January 5 order. <u>See Opp.</u> 7-8. Although

It does not matter that the January 5 order is not denominated an injunction by its terms. This Court is "not bound by what a district court chooses to call an order, or even by a failure to give an order a particular name." <u>Negrete v. Allianz Life Ins.</u> <u>Co.</u>, 523 F.3d 1091, 1097 (9th Cir. 2008). Instead, the Court "look[s] to [the order's] substantial effect rather than its terminology." <u>Orange County Airport Hotel Assocs.</u> <u>v. HSBC Ltd.</u>, 52 F.3d 821, 825 (9th Cir. 1995). Thus, "in deciding whether an appeal is proper," this Court asks: "(1) does the order have the practical effect of the grant or denial of an injunction; (2) does the order have serious, perhaps irreparable consequences; and (3) is the order one that can be effectively challenged only by immediate appeal?" <u>Negrete</u>, 523 F.3d at 1097 (internal quotation marks omitted).

The district court's directive – compelling the Government to authorize disclosure of classified information when responsible Executive officials have concluded that such disclosure is inconsistent with national security – indisputably has the practical effect of an injunction. It compels a party to take action that is being withheld. And the district court has threatened serious, perhaps irreparable, consequences if the Government does not satisfy the mandate of the January 5 order.

plaintiffs would have the district court itself grant a need-to-know determination (which would support collateral order jurisdiction in this Court, as we have explained), the district court has not specified whether it intends to take that step, or whether, instead, it has compelled the Executive Branch to grant access to the classified information at issue.

At a minimum, such consequences include the threat of sanctions. 1/5/09 Order at 24 ("Failure to comply fully and in good faith * * * will result in an order to show cause re: sanctions."). More significantly, the district court (acting pursuant to its interpretation of FISA) may itself disclose classified information if the Executive does not authorize such disclosure. As explained, any such disclosure would be irreparable and would cause exceptionally grave harm to national security. Finally, the order's threat of imminent disclosure can only be effectively challenged by immediate appeal.

Plaintiffs argue that the injunctive aspect of the January 5 order – requiring the Executive Branch to authorize disclosure of classified information to plaintiffs' counsel – is not appealable because it is not "designed to accord or protect some or all of the substantive relief sought by a complaint." Opp. 8 (internal quotation marks omitted). That argument misconstrues both the order and the underlying claims. Plaintiffs' amended complaint seeks disclosure of "all unlawful surveillance of plaintiffs" and "all information and records * * relating to plaintiffs that were acquired through the warrantless surveillance program." Amended Compl. 15. Any such information, if it exists, would be highly classified and require security clearances to view. The district court's order directing the Executive Branch to grant such clearances is designed to accord or protect that relief.

Nor is it accurate to say that the January 5 motion's injunctive aspect "merely

regulates the conduct of the litigation by prescribing procedures to facilitate plaintiffs' showing of standing." Opp. 8 (citation and internal quotation marks The court's order is unlike the "exceptions to the reach of section omitted). 1292(a)(1)," as explained in Cohen v. Board of Trustees, 867 F.2d 1455, 1464 (3d Cir. 1989), cited in Orange County Airport Hotel, 52 F.3d at 825-26 (9th Cir. 1995). Those exceptions deal with purely procedural matters. See Cohen, 867 F.2d at 1464 ("an order entered against a party solely to enable another party to gain discovery," or "an order imposing the sanction of preclusion of evidence for failure to make discovery," or "an order staying or refusing to stay an action for equitable relief," or an "order[] attaching security for a judgment ultimately to be rendered"). Here, by contrast, the injunction directing the Executive to grant security clearances and authorize disclosure of classified information is directed at the ultimate questions plaintiffs seek to litigate, including the initial question of plaintiffs' standing. $\frac{5}{2}$

C. Mandamus.

Finally, if the Court has doubts about its appellate jurisdiction, we respectfully ask that the Court treat the Government's appeal as invoking this Court's mandamus jurisdiction. If there were no other avenue for immediate appellate review, the district

^{5/} Under § 1292(a)(1), this Court has jurisdiction to review the entire order, not just the propriety of injunctive relief. <u>Marathon Oil Co. v. United States</u>, 807 F.2d 759, 764 (9th Cir. 1986).

court's intention to disclose classified information over the objection of the Executive Branch would be subject to a writ of mandamus pursuant to 28 U.S.C. § 1651. Mandamus permits interlocutory review of privilege claims in such a circumstance. <u>See United States v. Austin</u>, 416 F.3d 1016, 1024 (9th Cir. 2005) (citing <u>United States</u> v. Amlani, 169 F.3d 1189, 1193 (9th Cir. 1999)).

This Court considers five factors in determining whether to grant mandamus:

(1) The party seeking the writ has no other adequate means, such as direct appeal, to attain the relief he or she desires. (2) The petitioner will be damaged or prejudiced in a way not correctable on appeal (3) The district court's order is clearly erroneous as a matter of law. (4) The district court's order is an oft-repeated error, or manifests a persistent disregard of the federal rules. (5) The district court's order raises new and important problems, or issues of law of first impression.

<u>Austin</u>, 416 F.3d at 1024 (internal quotation marks omitted). Those factors are demonstrably satisfied here. If the Court were to conclude that the January 5 order is not appealable as a collateral order or an injunction, there would be no other adequate means to attain relief. And, we have explained above and in our stay motion that the court's planned disclosure of classified information both would result in irreparable injury to the United States, including exceptionally grave harm to national security, and is erroneous as a matter of law. The district court's disregard of the governing executive orders and the Executive's constitutional responsibility and authority to safeguard national security information warrants a writ of mandamus.

It is of no moment that the Government's notice of appeal was not itself

denominated as a mandamus petition. This Court may treat this appeal as a petition for a writ of mandamus, or as a motion for leave to file such a petition. <u>See, e.g.,</u> <u>United States v. Bertoli</u>, 994 F.2d 1002, 1011-15 (3d Cir. 1993) (treating appeal as a petition for writ of mandamus or prohibition). There is no authority for plaintiffs' argument that a more formal step is necessary here. <u>See</u> Opp. 9-10.^{6/}

CONCLUSION

This Court should stay district court proceedings that will lead to disclosure of classified information, and plaintiffs' motion to dismiss should be denied.

Respectfully submitted,

MICHAEL F. HERTZ Acting Assistant Attorney General

DOUGLAS N. LETTER THOMAS M. BONDY H. THOMAS BYRON III Attorneys, Appellate Staff Civil Division, Room 7513 Department of Justice 950 Pennsylvania Ave., N.W. Washington, D.C. 20530-0001 202-514-3602

FEBRUARY 2009

⁶/ If this Court concludes that a more formal invocation of the Court's mandamus jurisdiction is required, the Government is prepared to submit a separate petition.

CERTIFICATE OF SERVICE

I hereby certify that on February 25, 2009, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system. I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Lisa R. Jaskol 610 S. Ardmore Ave. Los Angeles, CA 90005 (213) 385-2977 ljaskol@earthlink.net Thomas H. Nelson 24525 E. Welches Road Welches, OR 97067 (503) 622-3123 nelson@thnelson.com

J. Ashlee Albies Steenson, Schumann, Tewksbury, Creighton & Rose, P.C. 815 S.W. Second Ave. Portland, OR 97204 (503) 221-1792 ashlee@sstcr.com

H. Thomas Byron III Attorney

Case 8:07ec090110396/RV02/2D/acumentF6092: 1 dFilled 01/019/2009: 68721973 of 10

1	GREGORY G. KATSAS
2	Assistant Attorney General, Civil Division JOHN C. O'QUINN
3	Deputy Assistant Attorney General DOUGLAS N. LETTER
	Terrorism Litigation Counsel
4	JOSEPH H. HUNT Director, Federal Programs Branch
5	ANTHONY J. COPPOLINO Special Litigation Counsel
6	ALEXANDER K. HAAS
7	Trial Attorney U.S. Department of Justice
8	Civil Division, Federal Programs Branch 20 Massachusetts Avenue, NW, Rm. 6102
	Washington, D.C. 20001
9	Phone: (202) 514-4782—Fax: (202) 616-8460
10	Attorneys for the Government Defendants
11	
12	UNITED STATES DISTRICT COURT
13	NORTHERN DISTRICT OF CALIFORNIA
14) No. M:06-CV-01791-VRW IN RE NATIONAL SECURITY AGENCY)
	TELECOMMUNICATIONS RECORDS) DECLARATION OF ARIANE E.
15	LITIGATION) CERLENKO, NATIONAL SECURITY) AGENCY, IN SUPPORT OF
16	This Document Solely Relates To: DEFENDANTS' MOTION FOR A STAY PENDING APPEAL AND FOR
17	Al-Haramain Islamic Foundation et al.) CERTIFICATION OF AN
18	v. Bush, <u>et al</u> . (07-CV-109-VRW)) INTERLOCUTORY APPEAL
19) Honorable Vaughn R. Walker
	}
20	I, Ariane E. Cerlenko, do hereby state and declare as follows:
21	1. I am the Associate General Counsel for Litigation in the Office of General
22	
23	Counsel for the National Security Agency (NSA). The Office of General Counsel ("OGC") is
24	responsible for providing legal services to the Director of the NSA and to all subordinate NSA
	officials and elements. I oversee a staff of fifteen (15) attorneys, paralegals, and office support
25	personnel. I have served in this position since July 2003, first in an acting capacity and, since
26	September 2004, as the permanent head. Prior to that time, I served as the Assistant General
27	
28	Declaration of Ariane E. Cerlenko in Support of Government Defendants' Motion for a Stay Pending Appeal and for Certification of Interlocutory Appeal <i>Al-Haramain v. Bush</i> (07-cv-109-VRW) (MDL06-cv-1791-VRW)

Case 3:07ecv000100364/RV02/20/000entFore 2: 2 dFiled 01/010/2009: 682age 2 of 10

Counsel of Civil Litigation from July 2000 to July 2003, where I was primarily responsible for the conduct of civil litigation matters for the NSA.

1

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

2. In my capacity as the Associate General Counsel for the Litigation Division, I am responsible for oversight of NSA involvement in all civil and criminal litigation matters. I have been responsible for the NSA's oversight of this litigation since its inception, working directly with Department of Justice litigation counsel and supervising attorneys in the OGC who are assisting in this matter. I have reviewed the content of public and classified declarations filed by NSA officials in this action, including by the Director of the NSA, Lt. Gen. Keith Alexander. I also have read the Court's Order of January 5, 2009. The purpose of this declaration is to summarize the process under which an individual may be granted access to classified NSA information. As set forth below, under these procedures, even if a person is found to be suitable to receive access to classified information, the agency that originates classified information would retain authority to make a separate determination on whether that person has a "need to know" and may in fact be granted access to its classified information. In addition, subsequent to the Court's January 5, 2009 Order, the NSA Director has reviewed the matter and has determined that the plaintiffs' counsel do not have the requisite "need to now" and therefore should not receive access to the NSA information at issue in this case.

A.

4.

Security Clearance and Access Process

3. The President of the United States, through the authority vested in him by the Constitution and the laws of the United States, has prescribed procedures governing access to classified information. Specifically, through Executive Orders issued by the President, a uniform system of classifying, safeguarding, and declassifying national security information has been created. *See* Exec. Order No. 12,958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Exec. Order No. 13,292, 68 Fed. Reg. 15315 (Mar. 25, 2003); *see also* Exec. Order 12,968, 60 Fed. Reg. 40,245 (Aug. 2, 1995) (establishing a uniform Federal personnel security program for employees who will be considered for access to classified information).

26 27

Pursuant to the Executive Order, all applicants seeking access to classified NSA

28 Declaration of Ariane E. Cerlenko in Support of Government Defendants' Motion for a Stay Pending Appeal and for Certification of Interlocutory Appeal *Al-Haramain v. Bush* (07-cv-109-VRW) (MDL06-cv-1791-VRW)

-2-

Case 8:07ecv90(150964/RV02/2D/0cu09entF60g2: 3 dFiled 01/01/2009: 682ag7 3 of 10

information must complete a two-step process. *See* Exec. Ord. 12958 § 4.1. One step is that a person must receive a favorable determination of eligibility for access to classified information. *Id.* at § 4.1(a)(1). This is also referred to as a "suitability" determination. In this case, the process for determining the suitability of plaintiffs' counsel to receive classified information would be overseen by officials with the United States Department of Justice who are responsible for ensuring the security of classified information in court proceedings. After a background investigation, DOJ security officials would determine if plaintiffs' counsel are eligible for a security clearance at a particular level (*i.e.*, Confidential, Secret, or Top Secret). *See* Exec. Ord. 12958, § 1.2 (describing levels of clearances).

5. A favorable eligibility or "suitability" determination, and the granting of a security clearance, does not mean that a person may receive access to classified information, but only that they are eligible to receive such information. In order to receive actual access to classified information, separate approval by the Executive Branch department or agency that controls the information is also necessary. Specifically, the originating agency must separately determine whether an individual has a "need to know" certain classified information. *See* Exec. Ord. 12958 §§ 4.1(a)(3). A "need to know" classified information is defined as "a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." *See* Exec. Ord. 12958 § 6.1(z).

6. In addition, if the information at issue resides in a "special access program," access is further restricted and may only be granted in accordance with the procedures established by an agency head. *See* Exec. Ord. 12958 § 4.3. The Executive Order provides that the number of persons who will have access to special access programs "will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved." *Id.* § 4.3(b)(3). In addition, the Director of National Intelligence ("DNI") has promulgated an Intelligence Community (IC) Directive that concerns special access programs that govern access to particularly sensitive information concerning intelligence related matters

Declaration of Ariane E. Cerlenko in Support of Government Defendants' Motion for a Stay Pending Appeal and for Certification of Interlocutory Appeal *Al-Haramain v. Bush* (07-cv-109-VRW) (MDL06-cv-1791-VRW)

-3-

Case 8:07ecv000150956/RV02/25/00009entF8092: 4 dFiled 01/010/2009: 682age 3 of 10

referred to as "Sensitive Compartmented Information" ("SCI"). *See* ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" (Attachment A). Under ICD 704, "the DNI retains the authority in any case to make a determination granting or denying access" to SCI information and "all such determinations are discretionary and based on [Intelligence Community] mission requirements, and do not create any rights, substantive or procedural." *Id.* at 1-2.

7. If the NSA decides to grant access to classified NSA information, the individual obtaining access must first undergo an orientation process (known as a "read in"). The purpose of the read in process is to describe facts concerning the compartmented activity so that the person being granted access is generally familiar with the nature of the classified information in the compartment, why that information is classified, the harm to national security that would result from disclosure of information contained in the compartment, and the specialized handling and storage restrictions and any additional requirements that apply to information in the compartment. Thus, the read in process itself entails the disclosure of classified information. Access to information residing in the compartment cannot occur prior to the "read in" described above. In addition, even after an individual has been "read in" to a particular program, NSA continues to control the particular information provided to that individual based upon the individual's need to know.

B.

Access to NSA Information in this Case

8. In this case, the NSA decided to provide classified information directly to the Court for *ex parte*, *in camera* review in connection with the state secrets privilege assertion made by the DNI in this case. These submissions set forth classified information related to the functions and activities of NSA and were classified at the TOP SECRET/SCI level and contain information concerning the Terrorist Surveillance Program, which is an NSA special access program. This information was not intended to be shared with the plaintiffs' counsel, but to assist the Court in deciding the Government's state secrets privilege assertion.

Declaration of Ariane E. Cerlenko in Support of Government Defendants' Motion for a Stay Pending Appeal and for Certification of Interlocutory Appeal *Al-Haramain v. Bush* (07-cv-109-VRW) (MDL06-cv-1791-VRW)

-4-

Case 8:07ecv090150956/RV02/25/00009entF8092: 5 dFiled 01/010/2009: 682age 3 of 10

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

9. Under the particular circumstances of this case, even if plaintiffs' counsel were to obtain a favorable suitability determination, the NSA Director has determined that neither plaintiffs nor their counsel have a need for access to classified NSA information that has been (or would be) excluded under the state secrets privilege assertion. This includes: the sealed document inadvertently disclosed by the Treasury Department in 2004, the fact of whether or not the plaintiffs have been subject to surveillance by the NSA under any authority, and any information concerning the operations of the Terrorist Surveillance Program authorized by the President after the 9/11 attacks. As indicated in the Government's state secrets privilege assertion, NSA has determined that the disclosure of this information would cause exceptional harm to national security. See Public and Classified Declarations of Lt. Gen. Keith Alexander, Director of the NSA filed in this action. The NSA Director has further determined that it does not serve a governmental function, within the meaning of the Executive Order, to disclose the classified NSA information at issue in this case simply to assist the plaintiffs' counsel in representing the interests of private parties who have filed suit against the NSA and who seek to obtain disclosure of information related to NSA intelligence sources and methods.

I hereby declare under penalty of perjury that the foregoing is true and correct. Executed this the 19th day of January 2009.

ARIANE E. CERLENKO

Declaration of Ariane E. Cerlenko in Support of Government Defendants' Motion for a Stay Pending Appeal and for Certification of Interlocutory Appeal *Al-Haramain v. Bush* (07-cv-109-VRW) (MDL06-cv-1791-VRW) Case 8:07ecv000150956/RV02/25/00009entF8092: 6 dFiled 01/010/2009: 682age 5 of 10

ICD 704

INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 704



PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION AND OTHER CONTROLLED ACCESS PROGRAM INFORMATION (EFFECTIVE: 01 OCTOBER 2008)

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002, as amended; Executive Order (EO) 12333, as amended; EO 12958, as amended; EO 12968, EO 13467, and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Directive (ICD) establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs. This directive also documents the responsibility of the DNI for overseeing the program producing these eligibility determinations. It directs application of uniform personnel security standards and procedures to facilitate effective initial vetting, continuing personnel security evaluation, and reciprocity throughout the Intelligence Community (IC). This directive rescinds Director of Central Intelligence Directive 6/4, 02 July 1998, as amended; Intelligence Community Policy Memorandum (ICPM) 2006-700-3, 12 July 2006; ICPM 2006-700-4, 12 July 2006; ICPM 2006-700-5, 12 July 2006; and ICPM 2006-700-6, 12 July 2006.

C. APPLICABILITY: This directive applies to the IC, as defined by the National Security Act of 1947, as amended; and other departments or agencies that may be designated by the President, or designated jointly by the DNI, and the head of the department or agency concerned, as an element of the IC or those government entities designated to determine eligibility for SCI access.

D. POLICY

1. The DNI establishes eligibility standards for access to SCI and other controlled access program information. The DNI delegates to Heads of IC Elements the authority to grant access to such information in accordance with this directive. Heads of IC Elements may further delegate determination approval authority to the Cognizant Security Authority (CSA). Notwithstanding this delegation, the DNI retains the authority in any case to make a determination granting or denying access to such information. All such determinations are

ICD 704

discretionary and based on IC mission requirements, and do not create any rights, substantive or procedural.

2. In all access determinations, national security must be protected. Exceptions to the personnel security standards in this directive shall be based on a finding that the risk to national security is manageable and acceptable. Nothing in this directive, or its accompanying procedural guidelines, shall preclude the DNI, or Principal Deputy DNI, in consultation with the relevant Head of an IC Element, from taking actions regarding a subject's access to SCI and other controlled access information.

3. IC elements using polygraph programs for personnel security purposes may require polygraph examinations when the Head of an IC Element deems it to be in the interest of national security. These polygraph programs shall include standardized training and certification of operators to ensure consistent and fair processes.

4. Heads of IC Elements or designees may determine that it is in the national interest to authorize temporary access to SCI and other controlled access program information, subject to the following requirements -- temporary access approvals shall be granted only during national emergencies, hostilities involving United States personnel, or in exceptional circumstances when official functions must be performed, pursuant to EO 12968. Temporary access approvals shall remain valid until the emergency(ies), hostilities, or exceptional circumstances have abated or the access is rescinded. In any case, temporary access shall not exceed one year.

5. When eligibility for access is first adjudicated, CSAs are required to use sound risk management. Continuous personnel security and counterintelligence (CI) evaluation will be required of all personnel granted access to SCI and other controlled access program information.

6. Subjects who have immediate family members or other persons who are non-United States citizens to whom the subject is bound by affection or obligation may be eligible for access to SCI and other controlled access program information as the result of a condition, deviation, or waiver from personnel security standards.

This ICD and its associated Intelligence Community Policy Guidance (ICPG) promulgate the personnel security policy of the DNI. These associated ICPGs are described below:

a. The evolving critical threat environment requires that innovative security, CI, and risk management measures be continually developed and implemented to support intelligence production, information sharing, reciprocity, and personnel mobility. Eligibility for access to SCI and other controlled access program information shall be contingent on meeting DNI personnel security standards as measured by investigative activities prescribed in ICPG 704.1 and the application of specific adjudicative guidelines contained in ICPG 704.2.

b. Guidance pertaining to denial of initial access to SCI and other controlled access programs or revocation of continued access eligibility, and the appeals process for such actions is contained in ICPG 704.3.

c. All IC security elements shall accept in-scope personnel security investigations and access eligibility determinations that are void of conditions, deviations or waivers. Specific guidelines are contained in ICPG 704.4.

ICD 704

d. The IC Scattered Castles repository, or successor database, shall be the authoritative source for personnel security access approval verifications regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards. Heads of IC Elements shall ensure that accurate, comprehensive, relevant, and timely data are delivered to this repository. Specific guidelines are contained in ICPG 704.5.

e. Additional ICPGs, and amendments to the ICPGs listed above, may be promulgated by the Deputy Director of National Intelligence for Policy, Plans, and Requirements (DDNI/PPR) following formal IC coordination.

E. PERSONNEL SECURITY STANDARDS

Threshold criteria for eligibility for access to SCI are as follows:

1. The subject requiring access to SCI must be a U.S. citizen.

The subject must be stable, trustworthy, reliable, discreet, of excellent character, and sound judgment; and must be unquestionably loyal to the United States.

3. Members of the subject's immediate family and any other person(s) to whom the subject . is bound by affection or obligation shall not be subject to physical, mental, or other forms of duress by either a foreign power or by persons who may be or have been engaged in criminal activity, or who advocate either the use of force or violence to overthrow the U.S. Government, or alteration of the form of the U.S. Government by unconstitutional means.

F. EXCEPTIONS TO PERSONNEL SECURITY STANDARDS

I. A Head of an IC Element may grant access based on a condition, deviation, or waiver to the above standards based on all available information that the specific risk to national security is manageable and acceptable. In such cases, additional personnel security and/or CI evaluation may be required. All risk assessments shall become a part of an individual's security file and the results of the risk assessment shall be annotated as an exception in the record.

The DNI, or designee, is the exclusive authority for granting an exception to the requirement that the subject be a U.S. citizen. Exceptions to this requirement shall require a letter of compelling need that is based upon specific national security considerations.

3. When an exception to these personnel security standards is warranted and a subject is granted access to SCI and other controlled access program information, the approving organization shall document its findings in the subject's security record and the Scattered Castles or successor database. The findings shall be characterized as a waiver, condition, or deviation.

G. RESPONSIBILITIES

 Deputy Director of National Intelligence for Policy, Plans, and Requirements is responsible for enforcing the authorities and carrying out the responsibilities of the DNI with respect to security.

 Assistant Deputy Director of National Intelligence for Security is responsible for overseeing IC security programs. Case 3:07ecv9015096/RV02/25/0009entF80g2: 9 dFilled 01/019/2009: 682age 9 of 10

ICD 704

 Director of the DNI Special Security Center is responsible for developing, coordinating, and implementing DNI security policies throughout the IC and providing IC security services in the form of research, training, and security databases.

 Heads of IC Elements are responsible for uniformly and consistently implementing DNI security policies governing access to classified national intelligence.

5. Cognizant Security Authority is responsible, as the senior security authority designated by a Head of an IC Element, for overseeing all aspects of security program management within an organization. The CSAs may formally delegate responsibility for certain security matters to specific elements within their agencies.

H. EFFECTIVE DATE: This ICD is effective on the date of signature.

Director of National Intelligence

Date

OCT 08

Case 3:37ecv900150356/RW2/25020009entF80g2: 10Fifeb001/119/21009y: 682d6713 of 10

ICD 704

APPENDIX A - ACRONYMS

ICD 704 -- PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION AND OTHER CONTROLLED ACCESS PROGRAM INFORMATION

CI	counterintelligence
CSA	Cognizant Security Authority
DNI	Director of National Intelligence
EO	Executive Order
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
ICPM	Intelligence Community Policy Memorandum
SCI	Sensitive Compartmented Information
US	United States

5