Rita Siemion (Admitted *pro hac vice*)
C/O **THE CONSTITUTION PROJECT**
1200 18th Street NW, Suite 1000
Washington, DC 20036
PHONE: (202) 580-6920
EMAIL: RITASIEMION@GMAIL.COM

Counsel for Amicus Curiae

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION

Ayman Latif, et al., Plaintiffs, v. Eric H. Holder, Jr. et al., Defendants.	No. 3:10-cv-750-BR

BRIEF OF AMICUS CURIAE THE CONSTITUTION PROJECT IN SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

Reports

Other Authorities

INTEREST OF THE AMICUS CURIAE

The Constitution Project (TCP) is a constitutional watchdog that brings together legal and policy experts from across the political spectrum to promote and defend constitutional safeguards. TCP's bipartisan Liberty and Security Committee, founded in the aftermath of September 11th, is comprised of policy experts, legal scholars, and former high-ranking government officials from all three branches of government. This diverse group makes policy recommendations to protect both national security and civil liberties, for programs ranging from government surveillance to U.S. detention. Based upon these reports and recommendations, TCP files *amicus* briefs in litigation related to these issues.

TCP's Liberty and Security Committee has published a report addressing the very issues currently pending before this Court. In *Promoting Accuracy and Fairness in the Use of Government Watch Lists,* committee members urged that "procedural safeguards and other measures to promote fairness are needed to protect us from the dangers posed by the use of watch lists."[1] In particular, the report notes that "[e]ven in situations where watch lists may be appropriate, the use of such lists may harm innocent persons either because they share a name with another individual who is appropriately included, or because such people are placed on lists despite a lack of evidence to warrant such treatment." To address these threats to civil liberties, the report recommends a series of reforms, including urging policymakers to adopt a mechanism providing individuals with

[1] Liberty & Sec. Comm., The Constitution Project, *Promoting Accuracy and Fairness in the Use of Government Watch Lists* 1 (2007) (hereinafter TCP Report), Report and list of signers *available at* http://www.constitutionproject.org/wp-content/uploads/2012/09/53.pdf.

"a fundamentally fair opportunity to challenge their inclusion on a watch list, on grounds of either mistaken identity or inadequate justification for inclusion."[2] Accordingly, TCP files this brief in support of Plaintiffs to urge this Court to find that such a process is both required by law and feasible to establish.

SUMMARY OF THE ARGUMENT

As several government reports have recognized, the Terrorist Screening Database that houses the No Fly List is overinclusive, riddled with errors, and lacks sufficient internal auditing and external oversight. As a result, there is a high risk that innocent individuals will be included on the List and denied personal liberties erroneously.

For those who believe they have been placed on the No Fly List in error, there is no effective way to get off. The only available process, the Traveler Redress Inquiry Program, merely allows travelers to complain about any difficulties they have had while traveling. The process does not provide individuals who have been denied boarding with notice of the reasons they are included on the No Fly List, or afford them an opportunity to respond to those reasons in order to clear their names. A meaningful redress system that complies with due process is essential to ensure that innocent individuals are not denied the freedom to travel.

The government, in this case and in others, has objected to providing additional process. The government claims that even after an individual is aware of his or her status, affording individuals with notice of the government's reasons for including an individual

[2] TCP Report at 5.

on the No Fly List, and a meaningful opportunity to contest those reasons, would harm national security and require the disclosure of classified information.

But it is possible and necessary to develop a robust redress system that complies with due process and does not threaten national security. In a variety of similar contexts, courts can, and routinely do, protect sensitive and classified security information without diluting individual rights. The courts' experiences in these other contexts may serve as models for this Court in how to provide individuals with the process to which they are entitled while addressing any legitimate national security concerns. Furthermore, providing the required meaningful process would reduce mistaken targeting of innocent individuals, resulting in a more accurate No Fly List overall. A more accurate list would, in turn, enable the government to focus its limited law enforcement resources where they are most needed—on tracking individuals with actual ties to terrorism. Thus, ensuring due process for travelers like Plaintiffs in this case would both protect individual liberties from erroneous deprivation and improve security for us all.

ARGUMENT

I. DHS TRIP IS INSUFFICIENT TO REDUCE THE HIGH RISK OF ERRONEOUS DEPRIVATION OF PERSONAL LIBERTY CREATED BY THE ERROR-PRONE NO FLY LIST.

The risk of erroneous inclusion on the No Fly List (also referred to as the "List") is high due to rampant data errors, overinclusiveness, and lack of sufficient quality control to correct these errors. The costs to individuals who are placed on the List erroneously can include significant deprivations of liberty, including the freedom to

travel by plane to, from, or within U.S. airspace.[3] Under the *Matthews v. Eldridge* balancing test, procedural due process requires consideration of whether there is a high risk of erroneous deprivation of an individual's interest such that due process requires implementation of greater or alternative procedures to reduce that risk than the procedures already provided. 424 U.S. 319, 335 (1976). The only currently available redress procedures, the Department of Homeland Security's Traveler Redress Inquiry Program ("TRIP" or "DHS TRIP"), provides no notice of the reasons why an individual may be listed, nor any meaningful way for travelers to challenge their inclusion on the List. DHS TRIP thus fails to protect against the high risk of error created by the grossly inaccurate watch list. Therefore, more effective redress procedures, including adequate post-deprivation notice and an opportunity to respond to the government's reasons for its action, are required by the Due Process Clause.

A. The Database Containing the No Fly List Is Error-ridden, Overinclusive, and Lacks Sufficient Quality Control Procedures.

The Terrorist Screening Database ("TSDB" or "Database"), which houses the No Fly List, is error-ridden and overinclusive, leading to thousands of individuals being placed or kept on the List by mistake. Unfortunately, the Terrorism Screening Center ("TSC"), which oversees the Database, lacks sufficient quality control mechanisms to correct these problems. As a result, there is a high risk that innocent individuals will be

[3] U.S. Dep't of Homeland Sec., Privacy Office, *Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(B) of the Intelligence Reform and Terrorism Prevention Act of 2004* (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.

included in the Database and deprived of their personal liberties without an adequate justification.

Defendants argue that the TSDB is "updated daily" to ensure protection against erroneous or unnecessary infringements of liberty. *See* Defs' Brief in Supp. of Mot. for Partial Summ. J., Dkt. No. 85-1, at 19 ("Defs' Brief"). But external government audits of the TSC and the TSDB nominations process have found that the TSDB is riddled with errors and that TSC lacks sufficient internal quality control procedures to ensure the accuracy of the Database.[4] The most recent external audit of the TSC uncovered that a staggering 38% of the tested records in the TSDB contained "errors or inconsistencies

[4] *See, e.g.*, U.S. Gov't Accountability Office, GAO-12-476, *Terrorist Watchlist: Routinely Assessing Impacts of Agency Actions since the December 25, 2009, Attempted Attack Could Help Inform Future Efforts* (2012), *available at* http://www.gao.gov/assets/600/591312.pdf ("2012 GAO Report"); U.S. Dep't of Homeland Sec., Office of the Inspector General, Report Number OIG-11-107, *DHS's Role in Nominating Individuals for Inclusion on the Government Watchlist and Its Efforts to Support Watchlist Maintenance* (2011), *available at* http://www.oig.dhs.gov/assets/Mgmt/OIG_11-107_Sep11.pdf ("2011 DHS Report"); U.S. Dep't of Justice, Office of the Inspector General, Audit Division, Audit Report 09-25, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices* (2009), *available at* http://www.justice.gov/oig/reports/FBI/a0925/final.pdf ("2009 DOJ Report"); U.S. Dep't of Homeland Sec., Office of the Inspector General, Report Number OIG-09-64, *Role of the No Fly and Selectee Lists in Securing Commercial Aviation* (2009), *available at* http://www.oig.dhs.gov/assets/Mgmt/OIGr_09-64_Jul09.pdf ("2009 DHS Report"); U.S. Dep't of Justice, Office of the Inspector General, Audit Division, Audit Report 08-16, *Audit of the U.S. Dep't of Justice Terrorist Watchlist Nomination Processes* (2008), *available at* http://www.justice.gov/oig/reports/plus/a0816/index.htm ("2008 DOJ Report"); U.S. Dep't of Justice, Office of the Inspector General, Audit Division, Audit Report 07-41, *Follow-Up Audit of the Terrorist Screening Center* iii (2007), *available at* http://www.justice.gov/oig/reports/FBI/a0741/final.pdf ("2007 DOJ Report"); U.S. Gov't Accountability Office, GAO-08-110, *Terrorist Watchlist Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List* (2007), *available at* http://www.gao.gov/assets/270/268006.pdf ("2007 GAO Report"). *See also*, *Ibrahim v.* 669 F.3d 983, 990 (9th Cir. 2012).

that were not identified through the TSC's quality assurance efforts."[5] The Department of Justice Office of the Inspector General ("DOJ OIG") also found that the TSC had not implemented the necessary quality assurance controls recommended in the previous audit report, issued two years earlier, to ensure that the TSDB's records were complete and accurate.[6] As a result, the OIG found that the TSC "continues to lack important safeguards for ensuring data integrity…"[7]

Another government report showed that eight percent of names that are cleared for removal from the Database do not in fact get removed.[8] Thus, the DOJ OIG found that "[d]espite being responsible for removing outdated or obsolete data from the TSDB, however, the TSC did not have a process for regularly reviewing the contents of the TSDB to ensure that the database does not include records that do not belong on the watchlist."[9] Even for those records that are eventually removed, the process takes months.[10] Indeed, the most recent audit found that due to resource limitations, only 500-1,000 record changes could be made per day and, as a result, "the status of many individuals was incorrectly shown on the TSA's No Fly and Selectee lists for a period of time."[11] The reality is that removing a name from the TSDB is a long and arduous

---

[5] 2007 DOJ Report at 31.
[6] 2007 DOJ Report at 13.
[7] 2007 DOJ OIG Report at iii (conclusions).
[8] 2009 DOJ Report at 36, 41 (noting that "these former subjects may still be unnecessarily screened or detained by frontline personnel who are still instructed to approach the individual as a known or suspected terrorist").
[9] 2007 DOJ Report at 17.
[10] 2009 DOJ Report at 36 (stating that the FBI took an average of 60 days to process removal of a name from the TSDB and that 72 percent of the removals were untimely).
[11] 2007 DOJ Report at 33. Although this 2007 report is the latest comprehensive audit of the TSC, more recent reports related to the terrorist watch list confirm that quality

process that requires either TSC or the original nominating agency to request the removal, followed by additional review by senior management, and then coordination between the nominating agency and the TSC Quality Assurance Team.[12]

The sheer number of records in the TSDB also leads to a high risk of error. The number of records in the TSDB has long since surpassed the one million mark.[13] These records correspond to over 400,000 distinct individuals who are included in the Database.[14] An additional 20,000 records, on average, are added to the Database every single month.[15] This exponential growth is in part the result of the troubling fact that the TSC accepts all but one percent of the records nominated for inclusion in the Database, without any rigorous standards for review or verification.[16] More records mean more misidentifications. As the Department of Homeland Security (DHS) acknowledged to the Government Accountability Office (GAO), "increasing the number of records that air carriers used to screen passengers would expand the number of misidentifications to unjustifiable proportions without a measurable increase in security."[17]

---

assurance, accuracy, and timeliness concerns persist. *See, e.g.*, 2011 DHS Report at 28, 49; 2012 GAO Report.

[12] 2007 DOJ Report at 32-33.

[13] 2009 DOJ Report at ii ("As of December 31, 2008, the consolidated terrorist watchlist contained more than 1.1 million known or suspected terrorist identities"); Peter Eisler, USA Today, *Terrorist Watch List Hits 1 Million*, Mar. 10, 2009, http://usatoday30.usatoday.com/news/washington/2009-03-10-watchlist_N.htm.

[14] 2009 DOJ Report at ii n.4.

[15] 2007 DOJ Report at iii; 2008 DOJ Report.

[16] 2007 GAO Report at 22. In addition, reports reviewing the accuracy of the nominations process in particular, including the 2011 report by the Department of Homeland Security Office of the Inspector General, have found that there is still a lack of "standardization" in the processes for nominating individuals to the TSDB and that "timeliness and quality challenges" remain. DHS 2011 Report at 28, 49.

[17] 2012 GAO Report at 17 (citing DHS officials).

A prior one-time review of the Database revealed that roughly 50 percent of the names on the No Fly List did not warrant inclusion, demonstrating a serious problem of over-inclusion in the nomination process.[18] While several thousand of those improperly included names were removed at the time—cutting the No Fly List in half—the List more than doubled again in 2010 during the months following the attempted bombing of Northwest Flight 253 on Christmas Day 2009.[19] In response to that incident, new watch-listing guidance was issued, which, among other changes, lowered the standards for nomination to the Database even more so that a name could be added based on a single tip from a single source.[20]

Multiple agencies have since "expressed concerns about the increasing volumes of information and the related challenges in processing this information."[21] In other words, the explosive growth in the number of records and individuals included in the TSDB creates a growing needle-in-the-haystack problem: with hundreds of thousands of names, aliases, and other identifying information to sort through and analyze, finding the individuals who pose a real threat to airline safety becomes that much more difficult as the size of the haystack increases.

As the Ninth Circuit has recently recognized, government audits show that "tens of thousands of travelers have been misidentified because of misspellings and

---

[18] 2007 DOJ Report at xiii, 31-33.
[19] 2012 GAO Report at 14.
[20] 2012 GAO Report at 28; Ellen Nakashima, *Terrorist Watch List: One Tip Now Enough to Put Name in Database, Officials Say*, Wash. Post, Dec. 29, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/29/AR2010122901584.html.
[21] 2012 GAO Report at 28.

transcription errors in the nomination process, and because of computer algorithms that imperfectly match travelers against the names on the list." *See Ibrahim v. Dep't of Homeland Sec.*, 669 F.3d 983, 990 (9th Cir. 2012). And, as the Ninth Circuit has also pointed out, an audit of the DHS TRIP process showed that a single major air carrier alone encountered an average of 9,000 erroneous terrorist watch list matches every single day. *Id.*

Due to the rapid growth of the Database and "the weak quality assurance process" the OIG also concluded that "the TSC is underestimating the time required to sufficiently review all watchlist records for accuracy."[22] This problem of rapid growth and weak quality assurance leads to more innocent individuals being deprived of their liberties due to errors in the Database. As the report notes, "inaccurate, incomplete, and obsolete watchlist information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity."[23] These "false positives adversely affect the traveling public, air carriers, and government because they occur in large numbers on a daily basis."[24]

But despite this high risk that individuals will be deprived of their liberties erroneously, the 2012 GAO Report showed that "no entity is routinely assessing governmentwide issues, such as how U.S. citizens and lawful permanent residents are being affected by screening or the overall levels of misidentifications that are

[22] 2007 DOJ Report at iii.
[23] 2007 DOJ Report at iii.
[24] 2009 DHS Report at 37.

occurring."[25] In other words, no government entity is even keeping track of how many people are being misidentified due to errors in the Database.

B. DHS TRIP Does Not Adequately Reduce the High Risk of Erroneous Deprivation of Individuals' Liberties.

The current redress procedures provided by DHS TRIP do not meet the basic minimum requirements of due process guaranteed by our Constitution, and these procedures are insufficient to protect against the inaccuracies of the TSDB. As the District Court for the Northern District of California has found, to burden the right to travel by plane based on inaccurate data without an effective means of redress to correct those inaccuracies would be unconstitutional:

> To deny this right…based on inaccurate information without an effective means of redress would unconstitutionally burden the right to travel…Without question, the government can bar anyone from boarding a plane who presents a risk of terror. **The government may not, however, bar a citizen or lawfully present alien from boarding a plane based solely or mainly…on grossly inaccurate information without affording an opportunity to challenge the basis for the denial.**

Ibrahim v. Dep't of Homeland Sec., No. C 06-00545 WHA, 2012 WL 6652362, *7 (N.D. Cal. Dec. 20, 2012) (emphasis added).[26] *See also* TCP Report at 3-5 (To satisfy constitutional due process requirements, individuals seeking to clear their names and have them removed from government watch lists must be afforded a "fundamentally fair opportunity to challenge their inclusion on a watch list.").

---

[25] 2012 GAO Report at 26-27.

[26] In *Ibrahim*, the district court was considering defendants' 12(b)(6) motion to dismiss, while in the case currently before this Court, Plaintiffs are at the summary judgment stage and have presented evidence to support their claims.

The DHS TRIP process fails to protect against erroneous deprivations of liberty because it fails to provide post-deprivation notice of the reasons an individual has been listed or an opportunity to challenge one's inclusion on the List. As discussed below, although pre-deprivation notice of inclusion on a watch list may not be appropriate, once individuals have been denied the right to fly and advised that they are included on the No Fly List, post-deprivation official notice should be required. However, the TRIP process is limited to filling out an online form that asks only for identifying information and a brief description of the "incident" the traveler wishes to complain about. The traveler is limited to checking a box next to a pre-determined list of "incident types" and an incident description box that allows less than two pages of explanation.[27] The limited information allowed on the form is then transmitted from DHS TRIP to TSC, which then makes a secret determination as to whether any action should be taken. The traveler receives only a letter from DHS that neither confirms nor denies the existence of any terrorist watch list records relating to the individual, nor discusses what, if anything, the government may have done to resolve the issue.

As the GAO noted in its May 2012 Report, "[t]he DHS TRIP redress application asks travelers to identify their areas of concern, but the information collected generally does not allow DHS TRIP officials to determine if individuals were misidentified as being on the watchlist."[28] And, as the Ninth Circuit also pointed out in *Ibrahim*, DHS

[27] Dep't of Homeland Sec. Traveler Redress Inquiry Program Online Complaint Form, https://trip.dhs.gov. (last visited Mar. 29, 2013).
[28] 2012 GAO Report at 46.

itself found that the TRIP process was ineffective at addressing the concerns of misidentified travelers:

> The 2009 DHS report was less charitable, concluding that the "TRIP website advises travelers that the program can assist them with resolving a range of travel difficulties. Our review of redress results revealed that **those claims are overstated**. While TRIP offers effective solutions to some traveler issues, it **does not address other difficulties effectively, including the most common—watch list misidentifications in aviation security settings**.

669 F.3d at 990 (emphasis added).

The limited and ineffective process offered by DHS TRIP at no point provides travelers with notice of the basis for their inclusion on the No Fly List, or even notice of whether they are on the List. *Ibrahim*, 669 F.3d at 990 (citing 2006 GAO Report at 31 & 2009 DHS Report at 89).

The DHS TRIP process also fails to provide travelers with any meaningful opportunity to contest the government's reasons for including them on the List. Such a process, "in which the Executive's factual assertions go wholly unchallenged or are simply presumed correct without any opportunity…to demonstrate otherwise falls constitutionally short." *Hamdi v. Rumsfeld*, 542 U.S. 507, 537 (2004) (plurality opinion); *id.* at 553 (Souter & Ginsburg, JJ.., concurring) ("It is not that I could disagree with the plurality's determination…that someone in Hamdi's position is entitled at a minimum to notice of the Government's claimed factual basis for holding him, and to a fair chance to rebut it before a neutral decisionmaker.").

II. THE GOVERNMENT CAN PROVIDE MEANINGFUL REDRESS PROCEDURES WITHOUT HARMING NATIONAL SECURITY.

The government can provide a constitutionally adequate process that affords travelers with post-deprivation notice and a meaningful opportunity to contest their

inclusion on the No Fly List without endangering national security. The Supreme Court has held that providing the basic core rights of notice and an opportunity to be heard "does not pose a sufficient threat to national security to trump these core due process rights." *Hamdi*, 542 U.S. at 535 (plurality opinion); *id.* at 553 (Souter & Ginsburg, JJ.., concurring).

Specifically, post-deprivation notice to individuals who have already been denied boarding and have already been told by government or airline officials that they are on the No Fly List, would not harm national security. Nor would meaningful redress procedures. Courts and government agencies routinely adjudicate individual rights in cases involving sensitive or classified information without jeopardizing national security.

Indeed, a variety of tools are available to our courts to protect such information from improper disclosure. And, ultimately, providing meaningful redress procedures will make us all safer by improving the accuracy of the TSDB, which will enable law enforcement to focus scarce resources on cases where there is a reasonable basis to suspect individuals of actual ties to terrorism.

A. Providing Post-Deprivation Notice to Travelers Who Have Been Denied Boarding and Informally Advised That They Are On the No Fly List Would Not Endanger National Security.

Post-deprivation notice to travelers who have been denied boarding on their flights would not endanger national security. Amicus recognizes that pre-deprivation notice could give rise to some of the various national security concerns raised by Defendants. *See* TCP Report at 5. In the watch list context, pre-deprivation notice would generally be self-defeating and could undermine the national security rationales that watch lists are designed to serve by tipping off would-be terrorists to their actual

vulnerabilities. TCP Report at 14, 29-30. As a result, unlike post-deprivation notice, Amicus agrees that pre-deprivation notice is an impracticable solution in the watch list context. TCP Report at 30.

But post-deprivation notice, after travelers have already been denied boarding and been informally advised by government or airline officials that they are on the No Fly List does not raise these concerns. For instance, the concern that notice of inclusion on the No Fly List would enable would-be terrorists to take steps to avoid detection and circumvent surveillance is simply inapplicable to travelers who have already been "tipped off" that they are on the List and are under scrutiny by law enforcement.

Each of Defendants' arguments that providing individuals with post-deprivation notice would harm national security were raised, and squarely rejected, by the United States District Court for the Northern District of Illinois in *Rahman v. Chertoff*. No. 05 C 3761, 2008 WL 4534407, *5 (N.D. Ill. Apr. 16, 2008), *rev'd on other grounds*, 530 F.3d 622 (7th Cir. 2008).[29] In that case, the plaintiffs also challenged their inclusion in the TSDB and, in response, the government argued that providing those plaintiffs with notice of the basis for their inclusion in the Database would harm national security. *Id.*

In rejecting the various national security arguments raised by the government in *Rahman*, the court explained that the government's generalized national security concerns were not implicated where under the specific facts of the case at hand the

[29] The Seventh Circuit reversed the district court's ruling solely on class certification grounds due to the lack of typicality of claims among class members and the difficulty of defining the class with specificity, holding that "Plaintiffs are entitled to relief that will redress any discrete wrong done them. That can be accomplished without certifying a class." *Rahman,* 530 F.3d at 627. The district court's rulings cited here remain good law and persuasive authority for this Court.

individual plaintiffs were *already alerted* to the fact that they were under government scrutiny. *Rahman,* 2008 WL 4534407 at *5-6. Like the Plaintiffs allege in the instant case, each of the plaintiffs in *Rahman* knew they were included in the TSDB because they had been stopped repeatedly at the border by authorities; the court therefore found that there was "little force to the argument that revealing their TSDB status will alert these plaintiffs for the first time that they have been under government scrutiny." *Id.* at *6.

The court explained that the "predicate assumption" of the government's argument that notice would enable a would-be terrorist to alter his conduct to avoid detection is that such an individual is not aware that he is the subject of an investigation. *Id.* As the court acknowledged, the government's argument "could have force in a situation where a person seeking to learn of his or her TSDB status had not been stopped at the border or had not otherwise been alerted to the fact that he is under investigation." *Id.* But that is not the case where individuals seek post-deprivation notice.

Similarly, the *Rahman* court rejected the government's related argument that informing a particular individual that he or she was *not* on the list would embolden that person, or his associates, to engage in terrorist activity. Yet Defendants' remake the same argument here: "Knowing which members of a terrorist group have escaped the attention of law enforcement and intelligence investigations will permit such groups to manipulate the system…and even provide an incentive for them to prepare for and commit an act of terrorism before coming to the attention of government authorities." Coppola Decl. ¶ 33. This argument makes little sense in cases where the travelers have already have been banned from airline travel and questioned by law enforcement

authorities, and can hardly be said to have "escaped the attention of law enforcement." Thus, the court in *Rahman* found it unlikely that such individuals, having come to the attention of authorities during multiple stops at the border, would interpret the notice that they were not on the list "as a green light for activity that might bring them back under government scrutiny" as the government argued. *Rahman,* 2008 WL 4534407 at *6 n.11.

Defendants here also argue that even if Plaintiffs have been told that they are on the No Fly List by government officials, such informal notice would not "diminish the risks of official disclosure." Def. Br. at 32 (citing Coppola Decl. ¶ 35 which states, "[t]o the extent that an individual's watchlist status is alleged to have been disclosed by… government personnel, that still does not justify displacing the non-disclosure policy, and in no way diminishes the risks of such a course."). Yet neither Defendants nor Coppola describe a single national security risk presented by "formal" notice that is not already presented by individuals learning they are on the List through denied boarding or by an informal statement by an FBI agent. In rejecting the government's claim that it would always categorically harm national security to confirm or deny a person's watch list status, the court in *Rahman* found it significant that the government had, as Plaintiffs similarly allege here, already disclosed information that would tend to confirm or deny a person's status in the TSDB. *Rahman,* 2008 WL 4534407 at *6 (finding that because the government had disclosed such information to members of Congress, it could not later argue that disclosing such information would be harmful to national security categorically).

Thus, Defendants raise not a single harm to national security that would result from providing post-deprivation notice to travelers. The general national security

concerns raised may apply to situations involving pre-deprivation notice to watch-listed individuals, but, as the district court in *Rahman* explained in detail, these concerns are not applicable in cases where the travelers have already been informally advised that they are on the List.

B. Courts Routinely Adjudicate Matters Implicating National Security Concerns and Involving Sensitive or Classified National Security Information Without Jeopardizing National Security.

In our constitutional system of checks and balances, our nation's courts are tasked with ensuring that the other branches of government comply with the requirements of our Constitution, including the right to due process of law. In fulfilling this role in our Constitutional scheme, courts routinely rule on matters involving sensitive or classified security information. And courts do so without jeopardizing our nation's safety.

Indeed, the Supreme Court rejected the argument, raised by Defendants here, that separation of powers principles mandate a circumscribed role for the courts where adjudicating an individual's rights implicates national security concerns:

> …we necessarily reject the Government's assertion that separation of powers principles mandate a heavily circumscribed role for the courts in such circumstances. Indeed, the position that the courts must forgo any examination of the individual case…cannot be mandated by any reasonable view of separation of powers, as this approach serves only to *condense* power into a single branch of government…Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.

Hamdi, 542 U.S. at 535-36 (plurality) (internal citations omitted). The Court further explained that it would turn our system of checks and balances "on its head" to deny a citizen the right to *challenge the factual basis* for his detention in court "simply because the Executive opposes making available such a challenge." *Hamdi*, 542 U.S. at 536-37.

The Supreme Court also stated unequivocally that district courts are fully equipped to handle the task of engaging in factfinding processes involving sensitive national security matters: "[w]e have no reason to doubt that courts faced with these sensitive matters will pay proper heed both to the matters of national security that might arise in an individual case and to the constitutional limitations safeguarding essential liberties that remain vibrant even in times of security concerns." *Id*. at 538-39. The Ninth Circuit expressed similar confidence in the ability of this Court to handle the discovery of any sensitive intelligence information in this very case. *Latif v. Holder*, 686 F.3d 1122, 1130 (2012) ("We also leave to the sound judgment of the district court how to handle discovery of what may be sensitive intelligence information."). This Court should reject Defendants' attempts to convince the Court that it has no authority to adjudicate an individual case simply because the Executive opposes such a challenge, or because sensitive or classified information may be raised.

Courts and administrative bodies routinely review sensitive or classified information when adjudicating individual rights in a variety of different contexts. Examples include the Guantánamo habeas cases, litigation under the Freedom of Information Act (FOIA), and criminal cases that utilize the Classified Information Procedures Act ("CIPA") to handle classified evidence. In addition, several administrative bodies review such information when adjudicating adverse security clearance determinations. This Court can draw on these various examples to develop a workable process that will satisfy the core elements of due process in this context while adequately addressing any of the security concerns that may arise. These models do not provide an exact blueprint for this Court to apply in this case, but they demonstrate that

the core elements of due process can be provided even when national security concerns are implicated.

In the Guantánamo habeas context, for example, the United States District Court for the District of Columbia has adjudicated over sixty habeas claims by Guantánamo detainees seeking to challenge the government's factual basis for designating them as enemy combatants after the Supreme Court's ruling in *Boumediene v. Bush*, 553 U.S. 723 (2008). Indeed, "this is a question that the federal courts have *routinely* been called to answer in the Guantánamo habeas cases."[30]

In hearing these detainee challenges, the D.C. District Court must review sensitive and classified evidence. *See, e.g., Boumediene*, 553 U.S. at 795-96. In holding in *Boumediene* that such habeas case can and should proceed, the Supreme Court explicitly recognized that such evidentiary issues will arise during the course of these habeas proceedings but that district courts are capable of accommodating the government's interest in protecting sources and methods of intelligence gathering without "impermissibly diluting" the protections to which detainees are entitled.

While affording detainees with the opportunity to challenge the factual basis for their designation, the district court utilizes appropriate measures to protect information that would endanger national security if revealed publicly, including protective orders, in camera proceedings, redactions, summaries of evidence, and other tools. These

---

[30] *Drones and the War on Terror: When Can the U.S. Target Alleged American Terrorists Overseas? Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (2013) (written testimony of Stephen I. Vladeck), *available at* http://judiciary.house.gov/hearings/113th/02272013_2/Vladeck%2002272013.pdf (emphasis in original).

protective measures allow the court to balance the detainees' right to due process with the government's need to protect national security. Indeed, whatever criticism may be directed at the habeas litigation based on other concerns, the habeas litigation model demonstrates the feasibility of affording the right to challenge the factual basis for government action, while protecting any sensitive or classified national security information.

Similarly, in the criminal context, federal courts routinely handle classified and sensitive evidence following the guidelines for handling such information in the Classified Information Procedures Act (CIPA). This procedural statute ensures the proper protection of classified information while enabling the prosecution to use such evidence in its case-in-chief and defendants to use such evidence in his or her defense. *See* 18 U.S.C. App. III (2012). CIPA's provisions balance the needs of both parties to utilize such evidence in the adjudication of the individual case with the national security concerns of the government in protecting such evidence from public disclosure. *See, e.g.*, *United States v. Anderson*, 872 F.2d 1508 (11th Cir. 1989); *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996). CIPA guides the court in utilizing protective orders (section 3), substitutions (section 6), and special security procedures (section 9) to protect classified evidence. 18 U.S.C. App. III. With CIPA's guidance, federal district courts across the nation have, without incident, handled hundreds of terrorism-related criminal prosecutions since 9/11, demonstrating the ability of district courts to handle sensitive and classified security information.[31]

[31] *See, e.g.,* Letter from Ronald Weich, Assistant Attorney Gen., to Patrick Leahy and Jeffrey Sessions, U.S. Senators, Regarding Statistics Relating to the Prosecution of

The security clearance context also provides several useful models demonstrating methods for providing notice and an opportunity to contest the factual basis for an adverse action, even when sensitive or classified evidence is involved. When a federal security clearance is denied or revoked, the employee or applicant may appeal that adverse decision through the particular agency's appeal process. Each agency provides its own redress process, covering a range of flexible options, but a common thread is that the employee is provided with a written notice that includes the reasons for the security clearance decision, access to the evidence upon which the adverse determination is based, to the extent permitted by national security concerns, and an opportunity to contest that information either in writing or before an Administrative Judge or other appeal panel. *See, e.g.*, 10 C.F.R. § 710.29 (2012); 28 C.F.R. § 17.47 (2012); 28 C.F.R. § 17.15 (2012).[32] The various agency regulations governing challenges to adverse security

---

Terrorism, Mar. 26, 2010, *available at* http://www.justice.gov/cjs/docs/terrorism-crimes-letter.html; *see also* Katerina Herodotou, Human Rights First Blog, *Let the Numbers Do the Talking: Federal Courts Work* (Jul. 12, 2012), http://www.humanrightsfirst.org/2012/07/12/let-the-numbers-do-the-talking-federal-courts-work/ ("In the hundreds of cases prosecuted since 9/11, federal courts have prevented the unauthorized disclosure of classified information, protected key constitutional rights, and even prosecuted 67 terrorism suspects captured abroad."); Richard B. Zabel & James J. Benjamin, Jr., *In Pursuit of Justice: Prosecuting Terrorism Cases in the Federal Courts* preface (2009), *available at* http://www.humanrightsfirst.org/wp-content/uploads/pdf/090723-LS-in-pursuit-justice-09-update.pdf ("The Classified Information Procedures Act (CIPA), although subject to being improved, is working as it should: we were unable to identify a single instance in which CIPA was invoked and there was a substantial leak of sensitive information as a result of a terrorism prosecution in federal court.").

[32] For a concise overview of the procedures utilized by various agencies, including the Department of Homeland Security, Department of Justice, Central Intelligence Agency, and the Department of Defense, see R. Scott Oswald, *Introduction to the Federal Security Clearance Process (Part 2): Denial or Revocation of Clearance*, Westlaw Journal Government Contract, Vol. 25, Issue 13 (Oct. 31, 2011), *available at*

clearance decisions make it clear that "some degree of transparency to facilitate effective challenges is possible even in the national security context." TCP Report at 35.

In Amicus' report on government watch lists, TCP's Liberty and Security Committee suggests that meaningful redress could be provided through a simple process comprised of an oral administrative hearing with the benefit of legal representation, and the availability of judicial review under a de novo standard with the government bearing the burden of proof. Providing the hallmark requirements of due process—notice and an opportunity to be heard—would, unlike the TRIP procedures, substantially reduce the risk that individuals will be deprived of their liberties erroneously.

As these various contexts illustrate, district courts are undeniably capable of "disentangling" sensitive information from nonsensitive information as an individual case unfolds. *See In re U.S.*, 872 F.2d 472 (D.C. Cir. 1989). The government can adopt procedures similar to those utilized in these examples in this context to provide a meaningful opportunity to challenge one's inclusion on the No Fly List without harming national security.

C. The Tools Routinely Used by Courts to Protect Sensitive and Classified Information Are Equally Adequate to Protect Such Information in this Context Without Diluting Due Process Rights.

The various tools readily available to courts for protecting sensitive and classified information, and used routinely in the contexts discussed above, are equally available and effective in this context. To protect any classified or sensitive national security information that may arise during the course of affording individuals post-deprivation

---

http://www.employmentlawgroup.net/News/Articles/Intro_To_Federal_Security_Clearance_Process.pdf.

notice of the reasons for their listing and an opportunity to be heard in an effective manner, courts may utilize such measures as protective orders, bench trials, discovery stipulations, security clearances, in camera proceedings, redactions, substitutions, and summaries of evidence. *See, e.g., In re U.S.*, 872 F.2d at 478 (describing various tools available to protect sensitive or classified information during litigation).

For example, in *National Council of Resistance of Iran*, the D.C. Circuit held that plaintiffs, two organizations designated as foreign terrorist organizations by the U.S. government, were entitled to post-deprivation notice of the reasons for the government's designation and an opportunity to challenge those reasons. 251 F.3d 192 (D.C. Cir. 2001). Where necessary, the court protected the classified evidence underlying the designation through ex parte in camera review. *Id.* To satisfy the notice component of due process, the court required the government to provide the plaintiff with the *unclassified* information upon which the determination was based, including the administrative record, as a substitute for the classified information. *Id.* at 208-09. To satisfy the hearing component, the court required that the plaintiffs be given, at a minimum, an effective opportunity to rebut either the unclassified evidence against them or in some other fashion be afforded the opportunity to negate the proposition that they are foreign terrorist organizations. *Id*. at 209. But the involvement of classified evidence did not prevent the court from requiring the government to provide the plaintiffs with the basic elements of procedural due process.

Similarly, in *Rahman v. Chertoff*, discussed above, the court utilized several precautions, where necessary, to protect classified security information. 2008 WL 4534407 at *2. For instance, the court reviewed certain classified materials in camera,

and in strictly controlled security conditions. *Rahman,* 2008 WL 4534407 at *2 n.4. The court also specifically addressed the concern raised by Defendants here that providing individuals with notice of the reasons for their placement on the No Fly List and a meaningful opportunity to contest those reasons would "put FBI sources and methods at risk…" Defs.' Br. at 27. The district court determined that any concerns about protecting sources and methods of investigation could be addressed sufficiently in a protective order that shielded such information from public disclosure. *Rahman*, 2008 WL 4534407 at *10 (granting defendants' motion for a protective order barring disclosure of certain information that "would reveal methods and sources of information.").

Notably, "information contained within the TSDB is sensitive but unclassified,"[33] making it even easier for this Court to ensure that Defendants' security concerns are adequately addressed. For instance, in *Ibrahim*, where the plaintiff also challenged her inclusion on the No Fly List, the district court recently ruled that plaintiff's counsel, who had been cleared to receive and review sensitive security information, could have access to such information. 2012 WL 6652362, at *8. However, the court also ensured that a protective order was in place and ruled that the plaintiff herself would not have access to the information. *Id*. The court also emphasized that no classified information was actually involved in adjudicating the plaintiff's challenge to her inclusion on the No Fly List. *Id.* ("No classified information is involved in this case. This deserves repetition—NO CLASSIFIED INFORMATION IS INVOLVED IN THIS CASE…") (emphasis in

[33] 2011 DHS Report at 8-9.

original). And, to the extent classified information were to arise in adjudicating the claims of other travelers, this Court may utilize the various tools, discussed above, that courts across the nation use everyday to handle classified evidence.

These tools enable this Court to address legitimate national security concerns, without denying due process rights.

D. Providing Meaningful Redress Procedures Will Make Watch Lists More Accurate, Which Will Improve Our National Security.

Providing travelers with meaningful redress procedures would improve the accuracy of our watch lists. To be meaningful, the opportunity to be "heard" would include the right for individuals to rebut the reasons for their inclusion on the No Fly List. Allowing individuals to exercise this right would aid the government in protecting national security by pointing out inaccuracies, errors, and misinformation in our watch list data. More accurate watch lists would enable law enforcement to focus scarce government resources on individuals reasonably believed to have ties to terrorism, thereby improving security for us all.

Both the United States government and its residents have strong interests in ensuring that people who pose genuine threats to our national security are denied entry to the United States or access to vulnerable networks and facilities—including flying over United States airspace. TCP Report at 12. Accurate and properly managed watch lists can be a useful law enforcement tool that may help focus surveillance on productive targets, and assist in the coordination of multi-agency efforts to track and thwart potential threats. *Id*. However, these interests are served only to the extent that watch lists are accurate. *Id.*

By failing to allow individuals sufficient process to demonstrate that they pose little or no risk to national security and have been included on the No Fly List by mistake, we make it more difficult for law enforcement officials to focus on the individuals who pose the greatest risk. "Mistaken targeting of individuals is not only unfair to the innocent, but it wastes the scarce resources available to pursue genuinely productive law enforcement and national security initiatives." TCP Report at 12.

In the information age, the vastness of our ever-expanding universe of intelligence data presents a significant challenge to protecting our national security given the limited resources available for analyzing that data. Particularly when our intelligence databases contains vast amounts of both relevant and irrelevant data, we increase our risk of failing to prevent an attack due to failure to "connect the dots" because law enforcement officers are diverted from more productive activities.[34] This "needle in the haystack" problem was evident, for example, in the failure to "collect and understand the intelligence we already had" on the would-be Christmas Day bomber Abdulmutallab, which would have revealed that he was planning an attack.[35]

---

[34] Jerome P. Bjelopera, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress* 15-16 (2011), *available at* http://digital.library.unt.edu/ark:/67531/metadc83930/m1/1/high_res_d/R40901_2011Dec28.pdf ("The goal of 'connecting the dots' becomes more difficult when there is an increasingly large volume of 'dots' to sift through and analyze…some have expressedconcerns about the risk of 'pipe clogging' as huge amounts of information are...gathered without apparent focus.").

[35] *See* Barrack Obama, Remarks by the President on Strengthening Intelligence and Aviation Security (Jan. 7, 2010) (transcript available at http://www.whitehouse.gov/the-press-office/remarks-president-strengthening-intelligence-and-aviation-security) (President reporting on the intelligence reviews into why the terrorist watch list system failed to predict the bombing attempt on Northwest Flight 253 to Detroit on Christmas Day 2009).

According to the May 2012 Report by the GAO, the TSDB nominating agencies "have expressed concerns about the increasing volumes of information and related challenges in processing this information" and that the increasing intake of information has impacted the ability of analysts to review the information.[36] At times, the volume of data exceeded the National Counterterrorism Center's ability to process the information.[37]

More accurate watch lists, including a more accurate No Fly List, would decrease these risks by reducing the size of the haystack that must be searched and analyzed in order to track individuals reasonably suspected of terrorist activity. As a result, law enforcement would be able to focus resources where they can be most productive: investigating individuals reasonably suspected of terrorist or other criminal activity. TCP Report at 21. As Secretary of Homeland Security Janet Napolitano recently stated, the government must be smart about how it uses "information and intelligence analysis to allow us to focus our time and energy on people and cargo that pose the greatest risk…In other words, if we're looking for a needle in the haystack, an approach that is risk-based allows us to start looking through a much, much smaller stack…"[38] Secretary Napolitano further emphasized that such an approach will both facilitate the lawful travel that drives our economic growth and keep our country more secure. *Id.*

---

[36] 2012 GAO Report at 10-11.
[37] *Id.*
[38] *See* Janet Napolitano, Prepared Remarks for Secretary of Homeland Security Janet Napolitano's Third Annual Address on the State of Homeland Security, The Evolution and Future of Homeland Security (Feb. 26, 2013) (transcript available at http://www.dhs.gov/news/2013/02/26/secretary-homeland-security-janet-napolitano%E2%80%99s-third-annual-address-state-homeland).

Providing travelers with meaningful process, as required by the Constitution, to challenge their inclusion on the No Fly List would increase the accuracy of the List and, as a result, improve security for us all.

CONCLUSION

For these reasons, Amicus urges this Court to grant Plaintiffs' motion for partial summary judgment.

Dated: April 2, 2013.

Respectfully submitted,

/s/ Rita Siemion
RITA SIEMION (Admitted *pro hac vice*)
C/O **THE CONSTITUTION PROJECT**
1200 18th Street NW, Suite 1000
Washington, DC 20036
PHONE: (202) 580-6920
EMAIL: RITASIEMION@GMAIL.COM

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that on April 2, 2013, a copy of the foregoing was filed electronically. Notice of this filing will be sent to all parties for whom counsel has entered an appearance by operation of the Court's electronic filing system. Parties may access this filing through the Court's system. I further certify that a paper copy marked "Judge's Copy" will be delivered to the Clerk's Office within three business days in compliance with LR 100-7. I certify that a copy of the foregoing has been served by ordinary U.S. Mail upon all parties for whom counsel has not yet entered an appearance electronically: None.

s/ Rita Siemion
Rita Siemion