DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Docket No. TSA–2007–28972

RIN 1652-AA48
Privacy Act of 1974: Implementation of Exemptions
Secure Flight Records

RIN 1652-ZA14
Privacy Act of 1974: System of Records
Secure Flight Records

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

By notice of proposed rulemaking ("NPRM")[1] and notice to establish a system of records ("SORN")[2] published on August 23, 2007, the Department of Homeland Security ("DHS"), Transportation Security Administration ("TSA") proposes to implement the "Secure Flight Records" system ("Secure Flight") and exempt portions of it from most of the protections provided by the Privacy Act of 1974. As described by TSA, Secure Flight will enable the agency to "receive passenger and certain non-traveler information from aircraft operators, conduct watch list matching, and transmit watch list matching results back to aircraft operators."[3]

The Electronic Frontier Foundation ("EFF") notes at the outset that TSA has favorably revised many aspects of the Secure Flight system since the agency announced the test phase of

---

[1] Notice of Proposed Rulemaking, 72 Fed. Reg. 48397 (Aug. 23, 2007).

[2] Notice to Establish System of Records, 72 Fed. Reg. 48392 (Aug. 23, 2007).

[3] Notice of Proposed Rulemaking, 72 Fed. Reg. 48356 (Aug. 23, 2007).

the program three years ago.[4] We believe that the following aspects of TSA's revised Secure Flight proposal are steps in the right direction:

- TSA will require travelers to submit only their full names when booking tickets, thus enabling them to choose whether or not to provide the government more extensive personal information for watch list matching.[5]

- TSA will destroy travelers' data within seven days after completion of travel provided that the data subjects were not identified as potential watch list matches.[6]

- TSA will not claim any Privacy Act exemptions for information provided directly by individuals when they make airline reservations or seek access to secured areas covered by the Secure Flight program.[7]

While EFF commends TSA for these positive measures, we nonetheless believe that the system continues to violate the intent of the Privacy Act and lacks fundamental assurances of due process because TSA's notices unnecessarily exempt certain information in the system from crucial safeguards intended to promote record accuracy and secure the privacy of certain individuals whose information is maintained within the system — protections that the Privacy Act is intended to provide. Among other things, TSA will be under no legal obligation to inform the public of the sources of records contained in the system or provide the ability to access and correct records that are irrelevant, untimely or incomplete. The system may also contain information that is unnecessary and wholly irrelevant to the determination of whether an individual poses a threat to aviation security.

Pursuant to the agency's notices, EFF submits these comments to address the substantial privacy issues raised by the proposed Privacy Act exemptions; to request that TSA provide

---

[4] *See* Notice to Establish System of Records, 69 Fed. Reg. 57345 (Sept. 24, 2004).

[5] 72 Fed. Reg. 48356, 48359.

[6] *Id*. at 48363.

[7] 72 Fed. Reg. 48397, 48399.

greater transparency about the sources of information in the system before adopting the proposed exemptions; and to urge TSA to provide an additional opportunity for public comment once additional information about Secure Flight has been made public.

Background

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel within the country. In *Saenz v. Roe*, the Court noted that the "constitutional right to travel from one State to another is firmly embedded in our jurisprudence."[8] Likewise, former DHS Deputy Secretary Admiral James Loy once observed that "the founding fathers . . . had mobility as one of the inalienable rights they were talking about."[9] For this reason, any governmental initiative that conditions the right to interstate travel upon the surrender of privacy rights requires serious scrutiny.

The government's attempts to impose information-based prescreening upon passengers seeking to exercise the right to travel within the United States have been controversial and unsuccessful over the years. For instance, the Computer Assisted Passenger Prescreening Program ("CAPPS II"), proposed in 2003, would have examined commercial and government databases to assess the risk posed by airline passengers.[10] The system understandably was the focus of concern within Congress[11] and among the general public[12] due to its constitutional

[8] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966) (internal quotation marks omitted).

[9] Testimony of Admiral James Loy before House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (May 6, 2003).

[10] Notice, 68 Fed. Reg. 2101 (Jan. 15, 2003).

[11] In Homeland Security appropriations bill (H.R. 2555), Congress blocked deployment of CAPPS II until the GAO studied the program's implications. The GAO's ensuing report found that seven of eight concerns voiced by Congress had not been addressed. General Accounting

implications and massive scope (which sought to collect information about tens of millions of individuals). It also engendered strong opposition abroad, where foreign governments and their citizens resisted the demands of the U.S. government to provide detailed air passenger data as a condition of flight into the United States.[13] Much of the controversy surrounding CAPPS II centered on the system's secrecy and the lack of public information concerning the manner in which the system would assess the security risks particular individuals are deemed to pose, as well as the types of data that TSA would use to make such assessments. When the General Accounting Office (now the Government Accountability Office) ("GAO") issued a report on CAPPS II at Congress's request in February 2004, the GAO concluded that TSA had failed to address concerns about, among other things, privacy and provision of adequate redress.[14]

After TSA abandoned CAPPS II in 2005, the agency introduced Secure Flight as a replacement. As envisioned by TSA, Secure Flight would have compared Passenger Name Records ("PNRs") against watch list information compiled by the Terrorist Screening Center

---

Office, *Aviation Security: Computer Assisted Passenger Prescreening Program Faces Significant Implementation Challenges*, GAO-04-385 (Feb. 2004) (hereinafter "GAO Report"). Congress's concern about CAPPS II was also evident in Press Release, Office of Senator Ron Wyden, Wyden Wins Commerce Committee Approval to Require Oversight of CAPPS II Airline Passenger Screening System (Mar. 13, 2003); Press Release, Office of Senator Patrick Leahy, Reaction of Senator Leahy to GAO's Report on Flaws in the CAPPS II Program (Feb. 13, 2004); Press Release, Senate Governmental Affairs Committee, Senators Collins, Lieberman Ask TSA: What Other Airlines Have Been Contacted and Asked for Passenger Information? (Apr. 14, 2004).

[12] Editorials on CAPPS II published in major newspapers included Editorial, *Safe Skies*, Washington Post, Mar. 21, 2003, at A12; and Editorial, *Airport Screening System More Minus Than Plus*, Atlanta Journal Constitution, Mar. 25, 2004, at 14A.

[13] *See, e.g.*, Sara Kehaulani Goo, *U.S., EU Will Share Passenger Records*, Washington Post, May 2004, at A02.

[14] GAO Report, *supra* n11.

("TSC"), including expanded "selectee" and "no fly" lists.[15] TSA also planned to try to identify "suspicious indicators associated with travel behavior" in passengers' PNR data, as well as explore the use of commercial data within the program.[16] Like CAPPS II, this early version of Secure Flight foundered due in part to privacy concerns.[17]

Unfortunately, the revamped Secure Flight continues to present some of the same problems as past TSA prescreening proposals. When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.[18] The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[19] Adherence to these requirements is critical for a system like Secure Flight.

I. Secure Flight Continues to Lack Adequate Transparency

In a second NPRM published concurrently with the two notices at issue in these comments, TSA professed a commitment to "providing transparency about the Secure Flight program."[20] However, TSA has done little to inform the public about the databases upon which

---

[15] Notice to Establish System of Records, 69 Fed. Reg. 57345, 57346 (Sept. 24, 2004).

[16] *Id*.

[17] *See* Marilyn Geewax, *Air Security Plan Delayed*, Atlanta Journal-Constitution, Feb. 10, 2006 at 1F; *Air Passenger Screening Plan Suspended Over Security Concerns*, San Jose Mercury News, Feb. 9, 2006.

[18] S. Rep. No. 93-1183, at 1 (1974).

[19] *Id*.

[20] 72 Fed. Reg. 48356, 48372.

Secure Flight may rely, aside from the TSC's Terrorist Screening Database ("TSDB"), which has had well documented problems.[21] Furthermore, in an effort to obtain the public release of additional information concerning the TSC's watch list matching operations, EFF submitted a Freedom of Information Act ("FOIA") request to the Federal Bureau of Investigation ("FBI"), which manages the TSC, on August 30, 2006. More than a year later, the FBI has not responded to the request. Because the TSDB continues to have serious shortcomings, and because the FBI has not provided any information about the current state of the TSDB, EFF urges TSA to delay implementation of Secure Flight until the public is able to verify that the TSDB has been significantly improved.

In addition to the TSDB, TSA intends to rely on other government databases to perform its watch list matching function. As TSA explains:

> In the course of carrying out the Secure Flight Program, TSA will review information from Federal Bureau of Investigation (FBI) systems of records and from systems of records of other law enforcement and intelligence agencies if necessary to resolve an apparent match to a Federal watch list. Thee may include classified and unclassified governmental terrorist, law enforcement, and intelligence databases, including databases maintained by the Department of Homeland Security, Department of Defense, National Counterterrorism Center, and FBI. Records from these systems are exempt from certain provisions of the Privacy Act because they contain law enforcement investigative information and classified information.[22]

It is unclear from this explanation which databases TSA intends to use within Secure

[21] 72 Fed. Reg. 48392, 48393. *See* Government Accountability Office, GAO-05-356, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed* 31 (March 2005); Department of Justice, Office of the Inspector General, Audit Division, Audit Report No. 05-27, *Review of the Terrorist Screening Center* 66 (June 2005); Department of Justice, Office of the Inspector General Audit Division, Audit Report No. 07-41, *Follow-up Audit of the Terrorist Screening Center* ii (Sept. 2007). EFF will thoroughly discuss the TSDB's shortcomings in comments on an August 22, 2007 Federal Register notice, which announced the FBI's intention to expand that system.

[22] 72 Fed. Reg. 48392, 48393.

Flight, much less how individuals could possibly learn this information, since TSA proposes to exempt Secure Flight from 5 U.S.C. § 552a(e)(4)(I) (requiring agencies to publish the categories of sources of records in a system).[23] We thus believe that the public lacks sufficient information to fully comprehend what information Secure Flight would use to make assessments about people within the system, or what their rights would be with respect to information maintained in those various databases.

The continuing lack of transparency surrounding the interrelated screening systems underlying Secure Flight requires TSA to 1) delay implementation of the proposed Privacy Act exemptions for Secure Flight; 2) make additional details concerning the state of the consolidated watch list available to the public; and 3) provide further opportunity for public comment on Secure Flight once details about the underlying systems are revealed.

II. TSA's Bases For Claiming Privacy Act Exemptions for Secure Flight Contravene the Intent of the Privacy Act

The Privacy Act was passed to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[24] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[25]

---

[23] 72 Fed. Reg. 48397, 48399. TSA provides no explanation for claiming this exemption.

[24] Pub. L. No. 93-579 (1974).

[25] *Id.*

As an initial matter, TSA relies upon 5 U.S.C. §§ 552a(j)(2), (k)(1) & (k)(2) as the bases for its extensive Privacy Act exemption claims.[26] Each subsection raises different issues, which we address in turn.

First, subsection (j)(2) provides that a system of records may be exempted from certain provisions of the Privacy Act if the system is

> maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

Secure Flight, as described in TSA's August 23 notices, does not meet these criteria. None of the three specified categories of information accurately describes the personal data of the vast majority of the millions of law-abiding citizens affected by Secure Flight. Indeed, for the exemption to apply broadly to individuals in the system, TSA would effectively be asserting that millions of innocent citizens are "criminal offenders and alleged offenders," that those citizens are the subjects of "criminal investigation[s]," or that information concerning those citizens was "compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision." Indeed, it is clear that subsection (j)(2) does not contemplate a wholesale exemption for the system, but is intended to apply to

[26] 72 Fed. Reg. 48397, 48398.

individuals who are the specific subjects of criminal investigation or enforcement.[27] To the extent that this rationale is used to justify any greater exemption, its invocation is improper.

Second, subsection (k)(1) applies only where the system of records is "subject to the provisions of section 552(b)(1) of this section," *i.e.*, if the system contains officially classified information. TSA has designated the "Security Classification" of the system of records as "[u]nclassified; Sensitive Security Information."[28] Therefore, this system of records cannot be exempt under (k)(1).

Finally, subsection (k)(2) applies only where the system of records is "investigatory material compiled for law enforcement purposes," and further provides that

> if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual . . .

Given that TSA seeks to exempt portions of Secure Flight from the Privacy Act's access provisions, subsection (k)(2) does not authorize the agency's action. Undoubtedly, some individuals will be denied the right to travel (and many the right to travel free of unwarranted interference) "as a result of the maintenance of such material." In a speech delivered late last year, Secretary Chertoff discussed the consequences of an individual's name being on a "list," and explained that once the agency transmits a person's name to an airline, the carrier is

[27] "To the extent practicable, records permitted to be exempted from the [Privacy] Act should be separated from those which are not. Further, while the language permits agency heads to exempt systems of records, agencies should exempt only portions of systems whenever it is possible." Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28971 (July 9, 1975).

[28] 72 Fed. Reg. 48392, 48394.

"actually legally obliged to deny people the opportunity to fly."[29] Under such circumstances, the Privacy Act clearly requires the material to "be provided" to the affected individual.

In short, the rationales cited by TSA for claiming Privacy Act exemptions are limited, and can only possibly apply to a small number of the records in the system. The Privacy Act would therefore allow any exemptions discussed below to properly apply to only a very small percentage of the records in Secure Flight.

A. TSA's Notices Fail to Provide Meaningful Citizen Access to Personal Information

In its August 23 notices, TSA has exempted portions of Secure Flight from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;[30]
- the agency must publish a notice of the existence of records in the Federal Register, along with the categories of records maintained in the system, and the procedures an individual may follow to obtain notice of and access to a record maintained about him;[31] and
- the agency must, upon request, provide an individual with an accounting of disclosures about him that have been made to others.[32]

In place of the Privacy Act's access mandates, TSA has substituted a highly discretionary access procedure that makes TSA's Freedom of Information Act and Privacy Act Office

---

[29] Remarks by the Secretary of Homeland Security Michael Chertoff at the Federalist Society's Annual Lawyers Convention, November 17, 2006 (http://www.dhs.gov/xnews/speeches/sp_1163798467437.shtm).

[30] 5 U.S.C. § 552a(d)(1).

[31] 5 U.S.C. §§ 552a(e)(4)(G)-(I), (f).

[32] 5 U.S.C. §§ 552a(c)(3).

responsible for handling access requests.[33] An individual wishing to access her information contained in the system that "is not exempt from disclosure" must write to this office and provide her "full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury."[34] TSA's notices, however, fail to include any time line for the government to respond to requests, any guarantee that requests will even be considered or granted, or a right to appeal adverse determinations. If appropriate steps are followed to make an access request, an individual may be able to access information she provided directly to airline operators, but "Secure Flight will not make available information on the individual, such as watch list matching results or analyses that were not supplied by that individual."[35] Such limited, discretionary access is far weaker than the access provisions set forth in the Privacy Act, and TSA offers no explanation as to why such restricted access is necessary in the context of Secure Flight. TSA's substitute access provisions are in direct conflict with the goals of the Privacy Act, which is intended to provide citizens with a judicially enforceable right of access to personal information maintained by government agencies.

B. The Notices Do Not Provide Individuals Any Meaningful Redress in Secure Flight

A natural corollary to the right to access information is the right to correct it. However, TSA ignores the statutory right to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted portions of Secure Flight from the legal

[33] 72 Fed. Reg. 48392, 48396.

[34] *Id*.

[35] 72 Fed. Reg. 48397, 48398; Privacy Impact Assessment for the Secure Flight Program § 7.1 (Aug. 9, 2007) (emphasis added).

requirements that define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as:

- an agency must correct identified inaccuracies promptly;[36]
- an agency must make notes of requested amendments within the records;[37] and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[38]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[39]

Instead of the judicially enforceable right to correction set forth in the Privacy Act, however, TSA has established its own discretionary set of procedures for passengers to contest the accuracy of their records. TSA's notices state that the method for contesting records is to submit personal information and identification documents to the DHS Traveler Redress Program ("TRIP") — a process that remains unacceptably vague when, as the Privacy Act recognizes,

[36] 5 U.S.C. § 552a(d)(2)(B), (d)(3).

[37] 5 U.S.C. § 552a(d)(4).

[38] 5 U.S.C. § 552a(f)(4).

[39] H.R. Rep. No. 93-1416, at 15 (1974).

individuals should have the right to ensure the accuracy of information being used to make important determinations about them.[40]

Under the notice, TSA *may* correct erroneous information upon a passenger's request, but is not required to do so. Significantly, TSA has specifically exempted portions of the Secure Flight system of records from 5 U.S.C. § 552a(g), which grants the right to judicial review, as well as from access, correction, and relevance requirements.[41] In place of judicial review, DHS will provide a correction process that offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and can change at TSA's whim. It remains unclear what recourse a traveler has if he is identified as a potential watch list match through Secure Flight based on false or inaccurate information, especially if he cannot access the records that produced such a determination. Even worse, erroneous information about travelers could be maintained indefinitely in various databases, since Secure Flight information is available to others through thirteen routine uses.[42]

The fact that Secure Flight will draw much of its information from other systems of records makes the redress process even more Kafkaesque, because those systems may also be exempt from the protections of the Privacy Act. To illustrate the point, one need look no further than the FBI's TSDB. The TSC is a major data source feeding information into Secure Flight,[43] and yet provides absolutely no redress process for aggrieved individuals. In an August 22, 2007

---

[40] Privacy Impact Assessment for the Secure Flight Program §§ 7.1-7.2.

[41] 72 Fed. Reg. 48397, 48399.

[42] 72 Fed. Reg. 48392, 48395-6.

[43] 72 Fed. Reg. 48392, 48396; 72 Fed. Reg. 48397, 48398.

SORN for the Terrorist Screening Records System, which includes the TSDB, the FBI stated as follows:

> Because this system contains classified intelligence and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system are exempt from notification, access, and amendment [under] the Privacy Act (5 U.S.C. 552a).
>
> If, however, individuals are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, they may contact the Federal agency that is conducting the screening process in question ("screening agency"). . . . By contacting the screening agency with a complaint, individuals will be able to take advantage of the procedures available to help misidentified persons and others experiencing screening problems.[44]

Here, of course, the "screening agency" – TSA – has also exempted its system from the redress provisions of the Privacy Act. The government's handling of the redress issue is fundamentally dishonest and violates the most basic notions of due process.

C. TSA's Notice Fails to Assure Collection of Information Only for "Relevant and Necessary" Use

Finally, TSA has exempted portions of Secure Flight from the fundamental Privacy Act requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[45] This data collection approach plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of Secure Flight program on travelers. In adopting the Privacy Act, Congress was clear that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

[44] Notice to Amend System of Records, 72 Fed. Reg. 47073, 47078 (Aug. 22, 2007).

[45] 72 Fed. Reg. 48397, 48399.

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][46]

As the Office of Management and Budget noted in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[47]

The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection will spiral out of control unless it is limited to information that is likely to advance the government's stated (and legally authorized) objective. The "relevant and necessary" exemption will serve only to increase the likelihood that Secure Flight will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goals of expediting the pre-boarding process for travelers and improving transportation security.[48]

It is worth noting that in 2003, TSA gave notice of its plans to exempt CAPPS II from the "relevant and necessary" requirement.[49] The General Accounting Office, in a February 2004 report on CAPPS II to Congress, articulated serious concerns about this decision:

---

[46] S. Rep. No. 93-3418, at 47 (1974).

[47] 40 Fed. Reg. 28948, 28960.

[48] *See* Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).

[49] *Id*.

> These plans reflect the subordination of the *use limitation* and *data quality* practice (personal information should be relevant to the purpose for which it is collected) to other goals and raises concerns that TSA may collect and maintain more information than is needed for the purpose of CAPPS II, and perhaps use this information for new purposes in the future.[50]

(Emphasis in original.) In exempting portions of Secure Flight from the fundamental Privacy Act requirement that information collected about citizens be relevant and necessary for a given program, TSA could mislead the public about the scope and use of information collected, which is ostensibly intended to enhance aviation security and facilitate the pre-boarding process.

Conclusion

For the foregoing reasons, EFF believes that TSA must delay the implementation of its proposed Privacy Act exemptions for Secure Flight, and that the agency must provide the public more details about the system's sources of information prior to its implementation. We further urge TSA to provide an additional opportunity for public comment once this additional information about the system is made public.

September 24, 2007

Respectfully submitted,

Lee Tien
Marcia Hofmann
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

David L. Sobel
ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Ave. NW
Suite 650
Washington, DC 20009
(202) 797-9009

[50] GAO Report, *supra* n11 at 24.