BY FAX (202-224-1259 / 202-228-0303)

April 25, 2005

Chairman Ted Stevens
Co-Chairman Daniel K. Inouye
Senate Committee on Commerce, Science and Transportation
508 Dirksen Office Building
Washington, DC 20510

Dear Chairman Stevens and Co-Chairman Inouye,

We are writing on behalf of the Electronic Privacy Information Center ("EPIC") concerning the proposed Transportation Security Administration ("TSA") budget for Fiscal Year 2006. We would like to bring to your attention the significant increase in surveillance funding requested by TSA. We ask that this letter be included in the hearing record.

EPIC strongly opposes this increase in federal funding for TSA's surveillance programs. In its development and implementation of these surveillance programs, TSA has frustrated efforts to obtain openness and transparency under the Freedom of Information Act, and the agency has violated the spirit if not the letter of the Privacy Act. TSA also has shown a proclivity to using personal information for reasons other than the ones for which the information was gathered or volunteered. In addition, the public has had considerable difficultly with the agency's redress procedures. Furthermore, TSA has shown poor management of its financial resources.

We urge you to inquire what steps the agency will take to protect privacy and ensure transparency in data collection and use. We also urge you to scrutinize TSA's current redress procedures. Finally, we recommend against funding the Office of Screening Coordination and Operations.

President Bush's proposed budget would increase TSA spending by $156 million to $5.6 billion for FY 2006, but this increase is contingent upon $1.5 billion that will be generated by a 120% jump in security fees assessed to airline passengers.[1] Assistant Secretary David M. Stone defended the increase at the February 15, 2005, hearing before the Senate Committee on Commerce, Science and Transportation

[1] Transportation Security Administration Statement of Assistant Secretary David M. Stone Before the Committee on Commerce, Science & Transportation (Feb. 15, 2005).

saying air passengers, not the general public, should pay for air travel security.[2] However, this money will not go toward new security measures, but will replace funds now provided by the government for current air traveler security programs.[3]

Assistant Secretary Stone also testified that this increased fee would mean "resources from the general taxpayer could be used for more broadly applicable homeland security needs," but he did not define what these needs would be.[4] Other programs under TSA that are receiving an increase in funding in the proposed FY 2006 budget include surveillance programs that have significant privacy implications for tens of millions of American citizens and lawful foreign visitors.

When it enacted the Privacy Act, 5 U.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[5] 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[.]"[6]

The Supreme Court as recently as last year underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[7]

It is critical for TSA's programs to adhere to these requirements, as the program have a profound effect on the privacy rights of a large number of American citizens and lawful foreign visitors every year. However, TSA has failed to follow the spirit of the Privacy Act during development of these surveillance programs.

Recent Government Reports Show Problems Within TSA Programs

The Government Accountability Office ("GAO") and the Department of Homeland Security Inspector General last month released reports that were critical of

---

[2] *Id.* at 6.
[3] *Id.*
[4] *Id.*
[5] S. Rep. No. 93-1183, at 1 (1974).
[6] *Id.*
[7] *Doe v. Chao*, 540 U.S. 614, 618 (2004).

the Transportation Security Administration.[8] These reports highlight the agency's failures concerning privacy rights, transparency, and redress procedures.

The GAO's March report examined the Transportation Security Administration measures for testing the use of commercial data within Secure Flight, the agency's passenger prescreening program currently under development. The report, commissioned by Congress, found that the agency still has many issues to address before the viability of Secure Flight can be determined.[9] The GAO was unable to assess, among other things, the effectiveness of the system, the accuracy of intelligence data that will determine whether passengers may fly, safeguards to protect passenger privacy, and the adequacy of redress for passengers who are improperly flagged by Secure Flight.[10] The GAO specifically found that TSA "has not yet clearly defined the privacy impacts of the operational system or all of the actions TSA plans to take to mitigate potential impacts."[11]

TSA is requesting an increase of $49.3 million for its Secure Flight program to bring its FY 2006 budget to $94 million.[12] The Secure Flight passenger prescreening program could affect the tens of millions of citizens who fly every year, but in the creation of the program, TSA has frustrated efforts to obtain information under the Freedom of Information Act, and its actions concerning openness and transparency have violated the spirit of the Privacy Act**.**

Also in March, the Department of Homeland Security Inspector General issued findings on TSA's role in collecting and disseminating airline passenger data to third party agencies and companies. The report revealed that the agency has been involved in 14 transfers of data involving more than 12 million passenger records.[13] The Inspector General found, among other things, that "TSA did not consistently apply privacy protections in the course of its involvement in airline passenger data transfers."[14] Furthermore, TSA did not accurately represent to the public the scope of its passenger data collection and use.[15]

---

[8] Government Accountability Office, *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*, GAO-05-356 (March 2005) (hereinafter "GAO Report"). Department of Homeland Security Inspector General, *Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (Redacted)*, OIG-05-12 (March 2005) ("OIG Report").

[9] GAO Report, *supra* at 53. *See generally* EPIC's Secure Flight page *at* http://www.epic.org/privacy/airtravel/secureflight.html.

[10] GAO Report, *supra* at 53-62.

[11] *Id*. at 7.

[12] Department of Homeland Security, *Budget-in-Brief Fiscal Year 2006,* at 21 (Feb. 7, 2005) ("DHS Budget").

[13] OIG Report, *supra* at 6-7.

[14] *Id.* at 40.

[15] *Id*. at 42-48.

The Inspector General's critical report comes almost a year after the agency's admission that it had acted improperly with regard to passenger data collection and use. In June 2004 then-TSA Acting Administrator Admiral David Stone admitted to the Senate Governmental Affairs Committee that in 2002 TSA facilitated the transfer of passenger data from American Airlines, Continental Airlines, Delta Airlines, America West Airlines, Frontier Airlines, and JetBlue Airways to TSA "cooperative agreement recipients" for purposes of CAPPS II testing, as well as to the Secret Service and IBM for other purposes.[16] Stone also stated that Galileo International and "possibly" Apollo, two central airline reservation companies, had provided passenger data to recipients working on behalf of TSA.[17] Further, TSA directly obtained passenger data from JetBlue and Sabre, another central airline reservation company, for CAPPS II development.[18] TSA did not observe Privacy Act requirements with regard to any of these collections of personal information.[19] Stone's admission followed repeated denials to the public, Congress, GAO, and Department of Homeland Security Privacy Office that TSA had acquired or used real passenger data to test CAPPS II.[20] TSA exhibited a proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered.

Another example of TSA's failure to operate its programs with the openness and transparency necessary under the federal open government laws is its recent creation of an Aviation Security Advisory Committee Secure Flight Privacy/IT

---

[16] *See U.S. Senate Committee on Governmental Affairs Pre-hearing Questionnaire for the Nomination of Admiral David Stone to be Assistant Secretary of Homeland Security, Transportation Security Administration* 17, 19, *available at* http://www.epic.org/privacy/airtravel/stone_answers.pdf.

[17] *Id*.

[18] *Id*. at 19.

[19] *Id*. at 18.

[20] *See*, e.g., Ryan Singel, *More False Information From TSA*, Wired News, June 23, 2004 ("After the JetBlue transfer was brought to public attention in September 2003, TSA spokesman Brian Turmail told Wired News that the TSA had never used passenger records for testing CAPPS II, nor had it provided records to its contractors. In September 2003, Wired News asked TSA spokesman Nico Melendez whether the TSA's four contractors had used real passenger records to test and develop their systems. Melendez denied it, saying, 'We have only used dummy data to this point.' "); *U.S. Representative John Mica (R-FL) Holds Hearing on Airline Passenger Profiling Proposal: Hearing Before the Aviation Subcomm. of the House Transportation and Infrastructure Comm.*, 105th Cong. (March 2004) (Admiral Stone testifying that CAPPS II testing was likely to begin in June 2004); GAO Report at 17 ("TSA has only used 32 simulated passenger records – created by TSA from the itineraries of its employees and contractor staff who volunteered to provide the data – to conduct [CAPPS II] testing"); Department of Homeland Security Privacy Office, *Report to the Public on Events Surrounding jetBlue Data Transfer* (Feb. 2004) 8 ("At this time, there is no evidence that CAPPS II testing has taken place using passenger data").

Working Group. It appears to EPIC that, based upon the little public information that is currently available, the working group is subject to the Federal Advisory Committee Act ("FACA"), 5 U.S.C. App. 1, which includes the requirement that the working group publish notices of their meetings in the Federal Register. However, the formation of this working group was not announced in the Federal Register, and neither TSA nor the Department of Homeland Security has publicly acknowledged its existence or defined its mission. EPIC sent a letter in January to TSA's privacy officer, Lisa Dean, to ask for an explanation as to why this working group is not operating with the transparency and openness required under FACA.[21] In her March response letter, Ms. Dean advised us that Transportation Security Administration's position was that the work and materials of working group are subject to FACA.[22] The agency was noncommittal about the FOIA status of the material.[23]

TSA's Lapses in Public Accountability

The Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, establishes a legal right for individuals to obtain records in the possession of government agencies. The FOIA helps ensure that the public is fully informed about matters of public concern. Government agencies are obligated to meet the requirements of open government and transparency under the FOIA, but TSA has frustrated efforts to obtain information under the FOIA during the creation of these surveillance programs.

In September 2004, TSA announced plans to test the Secure Flight program. Secure Flight is intended to replace the now-defunct CAPPS II, but it includes many elements of the CAPPS II program, which was abandoned largely due to privacy concerns.[24] TSA said that "Secure Flight will involve the comparison of information for domestic flights to names in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC), to include the expanded TSA No-Fly and Selectee Lists, in order to identify individuals known or reasonably suspected to be engaged in terrorist activity."[25]

[21] Letter from David Sobel, General Counsel, EPIC, and Marcia Hofmann, Staff Counsel and Director, Open Government Project, EPIC, to Lisa Dean, Privacy Officer, Office of Transportation Security Policy, TSA, Jan. 31, 2005 (on file with EPIC).
[22] Letter from Lisa S. Dean, Privacy Officer, Office of Transportation Security Policy, TSA, to David Sobel, General Counsel, EPIC, Mar. 2, 2005 (on file with EPIC.)
[23] *Id.*
[24] *See* Sara Kehaulani Goo and Robert O'Harrow Jr., *New Screening System Postponed*, Washington Post, July 16, 2004, at A02.
[25] System of Records Notice, Secure Flight Test Records, 69 Fed. Reg. 57345 (Sept. 24, 2004).

On September 28, 2004, EPIC submitted a FOIA request to TSA asking for information about Secure Flight.[26] EPIC asked that the request be processed expeditiously, noting the intense media interest surrounding the program. Specifically, EPIC demonstrated that 485 articles had been published about the program since TSA announced its plans for Secure Flight. EPIC also mentioned the October 25, 2004, deadline for public comments on the test phase of the system, explaining the urgency for the public to be as well informed as possible about Secure Flight in order to meaningfully respond to the agency's proposal for the program. TSA determined these circumstances did not justify the information's immediate release, and refused EPIC's request that the information be made public prior to the October 25 deadline for these comments. TSA also denied EPIC a fee waiver, which the agency has never done before in its three-year existence. This maneuver imposed a significant procedural barrier to EPIC's ability to obtain the information. EPIC appealed TSA's decision, noting that the agency's actions were unlawful. Rather than defend its position in court, TSA has released a minimal amount of the information that EPIC requested. EPIC continues to seek from TSA information about the program that will affect tens of millions of airline passengers each year.

Problems With TSA Redress Procedures

The recently enacted Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA to create a system for travelers to correct inaccurate information that has caused their names to be added to the no-fly list.[27] TSA maintains that it has an adequate redress process to clear individuals improperly flagged by watch lists; however, it is well known that individuals encounter great difficulty in resolving such problems. Senators Ted Kennedy (D-MA) and Don Young (R-AK) are among the individuals who have been improperly flagged by watch lists.[28] Sen. Kennedy was able to resolve the situation only by enlisting the help then-Homeland Security Secretary Tom Ridge; unfortunately, most people do not have that option.

In March, Rep. Loretta Sanchez (D-CA) highlighted problems that everyday Americans have with the current TSA redress procedure. At a hearing of the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity concerning the proposed Fiscal Year 2006 budget, Rep. Sanchez reported that many of her constituents continue to face lengthy delays, questioning, and at times are

---

[26] Letter from Marcia Hofmann, Staff Counsel, EPIC, to Patricia Reip-Dice, Associate Director, FOIA Headquarters Office, TSA, Sept. 28, 2004 (on file with EPIC).

[27] P.L. No. 108-458 (2004).

[28] *See, e.g.*, Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Washington Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Richard Simon, *Iconic Senator Is Suspicious to Zealous Airport Screeners*, Los Angeles Times, Aug. 20, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press International, Aug. 20, 2004.

prohibited from boarding flights because they are misidentified as people sought on no-fly lists.[29] Her constituents continue to face these roadblocks even after they apply for, receive and then display to screener personnel the official federal government letters that establish their innocence. Rep. Sanchez questioned TSA officials about why current redress procedures have failed these American citizens. This issue remains important, as the GAO's March report examining Secure Flight found that "TSA has not yet clearly defined how it plans to implement its redress process for Secure Flight, such as how errors, if identified, will be corrected, particularly if commercial databases are used."[30]

TSA Has Violated the Spirit of Federal Privacy Laws

The proposed FY 2006 budget accords TSA's Registered Traveler program $22 million.[31] This is a pilot program TSA began conducting in July 2004 and is now operating at five airports.[32] The preliminary results are being examined by TSA to determine whether the program should be expanded to other airports. Registered Traveler allows frequent travelers to submit digital fingerprints, iris scans and undergo a background check in exchange for receiving a fast pass through the airport checkpoint. (The International Registered Traveler program was announced in January.) [33]

TSA first published a Federal Register notice about the program in June 2004.[34] In July 2004, EPIC submitted comments to address the substantial privacy issues raised by the Registered Traveler program and the new system of records established to facilitate the program.[35] EPIC requested that TSA substantially revise its Privacy Act notice prior to implementation of the final phase of Registered Traveler. TSA's subsequent Federal Register notice of the implementations of Privacy Act exemptions in the Registered Traveler program did not solve any the privacy right threats that EPIC highlighted in its comments.

---

[29] Shaun Waterman, *No Redress Mechanism in New DHS Terrorist Screening Office*, United Press International, Mar. 2, 2005.
[30] GAO Report, *supra* at 7.
[31] DHS Budget, *supra* at 21.
[32] Press Release, *U.S. Department of Homeland Security TSA, Secretary Ridge Unveils Registered Traveler Pilot Program At Reagan National Airport* (Sept. 3, 2004).
[33] Press Release, *U.S. Department of Homeland Security, Secretary Tom Ridge Announces Enhancement of Expedited Traveler Program Through New York's JFK Airport* (Jan. 13, 2005).
[34] Privacy Act Notice, 69 Fed. Reg. 30948 (June 1, 2004).
[35] Comments of the Electronic Privacy Information Center on Registered Traveler Operations Files Privacy Act Notice, June 1, 2004, *available at* http://www.epic.org/privacy/airtravel/rt_comments.pdf.

TSA's notice for the Registered Traveler system of records, however, exempts the system from many protections the Privacy Act is intended to provide.[36] As proposed in the notice, Registered Traveler is a program for which TSA is asking individuals to volunteer information that will be used to conduct potentially invasive background checks in exchange for the determination that they have a relatively low likelihood of being terrorists or connected to terrorists, and may be subject to less security screening than others prior to boarding airplanes. However, TSA has unnecessarily exempted the system from crucial safeguards intended to promote record accuracy and secure the privacy of individuals whose information is maintained within the system. TSA will be under no legal obligation to inform the public of the categories of information contained in the system or provide the ability to access and correct records that are irrelevant, untimely or incomplete. The program will contain information that is unnecessary and wholly irrelevant to the determination of whether an individual poses a threat to aviation security.

Questions Remain About the Transportation Worker Identity Credential Program

TSA is requesting $244 million for its pilot Transportation Worker Identity Credential program ("TWIC") for FY 2006.[37] TWIC is an identification card given to transportation workers, authorized visitors and all other persons requiring unescorted access to transportation infrastructure secure areas. The program is operating at 34 sites in six states, but TSA hopes to eventually extend the program to workers in all modes of transportation, which could encompass as many as 6 million people.[38] Persons required to have the identification card submit sensitive personal and biometric information to a central TSA database used to validate a person's eligibility to access these areas. EPIC submitted comments in November 2004 highlighting the dangers to travelers' privacy rights inherent in the program.[39] TSA has not released information clearly explaining to the public how it intends safeguard the sensitive personal information gathered on program participants. The lack of transparency and openness about TWIC is against the spirit of federal open government laws.

Another important reason not to increase the funding for TWIC is because TSA has not used its current funding judiciously. The GAO reviewed TWIC in December 2004, and found that because of program delays, some port facilities are forced to proceed "with plans for local or regional identification cards that may require additional investment in order to make them compatible with the TWIC system. Accordingly, delays in the program may affect enhancements to port security

[36] Privacy Act Notice, 69 Fed. Reg. 54256 (Sept. 8, 2004).
[37] DHS Budget, *supra* at 21.
[38] TSA's fact sheet on the Registered Traveler program, *available at* www.tsa.gov/interweb/assetlibrary/RT_Factsheet.pdf.
[39] Comments of the Electronic Privacy Information Center on Transportation Security Threat Assessment System and Transportation Worker Identification Credentialing System Privacy Act Notice, Sept. 24, 2004, *available at* http://www.epic.org/privacy/airtravel/twic_comments.pdf.

and complicate stakeholder's efforts in making wise investment decisions regarding security infrastructure."[40]

The financial problems encountered in TSA's TWIC program are emblematic of TSA's troubles managing its finances, according to the GAO. Cathleen Berrick, GAO Director of Homeland Security and Justice, told the Senate Committee on Commerce, Science & Transportation on February 15, 2005, that TSA had not always "conducted the systematic analysis needed to inform its decision-making processes and to prioritize its security improvements."[41] Examples include the fact that in FY 2005, TSA was forced to transfer about $61 million from its Research and Development budget of $110 million, to support its operations, such as personnel costs for screeners.[42]

A significant issue is that these surveillance programs are receiving substantial funding and TSA manpower while the current aviation program to screen passengers and their luggage for dangerous objects is woefully inadequate. Ms. Berrick reported at the February 15 hearing that there has been only modest progress in how well screeners detect threat objects following a report last year that documented gaps in screener security.[43] The increased funds that TSA has earmarked for surveillance programs can also be used in another important program: Threat Assessment of General Aviation. The GAO reported that "though the Federal Bureau of Investigation has said that terrorists have considered using general aviation to conduct attacks, a systematic assessment of threats has not been conducted."[44] TSA has cited cost as the reason that TSA has conducted vulnerability assessments at only a small number of the 19,000 general aviation airports nationwide.

Office of Screening Coordination and Operations Raises New Privacy Problems

The Department of Homeland Security ("DHS") has proposed the creation and funding of the Office of Screening Coordination and Operations ("SCO"), which would oversee vast databases of digital fingerprints and photographs, eye scans and personal information from millions of Americans and foreigners. This office would be responsible for United States-Visitor and Immigrant Status Indicator Technology (US-VISIT), Free and Secure Trade, NEXUS/Secure Electronic Network for Travelers Rapid Inspection, TWIC, Registered Traveler, Hazardous Materials Trucker Background Checks, and Alien Flight School Checks.[45] This mass compilation of personal information has inherent dangers to citizens' privacy rights

[40] Government Accountability Office, *Transportation Security: Systematic Planning Needed to Optimize Resources, Statement of Cathleen A. Berrick, Director Homeland Security and Justice*, GAO-05-357T (Feb. 15, 2005).
[41] *Id.* at 2.
[42] *Id.* at 31.
[43] *Id.* at 11.
[44] *Id.* at 17.
[45] DHS Budget, *supra* at 6.

and it is imperative that SCO fulfill its legal obligations for openness and transparency under the FOIA and Privacy Act.

According to the proposed FY 2006 budget, the mission of the proposed SCO is "to enhance the interdiction of terrorists and the instruments of terrorism by streamlining terrorist-related screening by comprehensive coordination of procedures that detect, identify, track, and interdict people, cargo and conveyances, and other entities and objects that pose a threat to homeland security."[46] The budget goes on to say that "the SCO would produce processes that will be effected in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by Federal law."[47] It is unclear, however, what steps the office intends to take to protect these rights.

There is a significant risk that the creation and funding of the SCO would allow for mission creep — a risk that the data collected and volunteered by airline passengers, transportation workers and foreign visitors will be used for reasons not related to their original aviation security purposes. Though TSA has stated that it will not use the sensitive personal data of tens of millions of Americans for non-aviation security purposes, TSA documents about the CAPPS II program collected by EPIC under the FOIA clearly show that TSA had considered using personal information gathered for CAPPS II for reasons beyond its original purposes. For example, TSA stated that CAPPS II personal data might be disclosed to federal, state, local, foreign, or international agencies for their investigations of statute, rule, regulation or order violations.[48] Again, TSA exhibited a proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered.

The Transportation Security Administration has frustrated efforts to ensure openness and transparency under the Freedom of Information Act and has violated the spirit of the Privacy Act for the protection of privacy rights in the development of the above programs. TSA also has shown a proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered. The agency's current redress procedures have failed to resolve valid grievances of innocent citizens flagged by the no-fly lists. TSA also has shown poor management of its financial resources. For these reasons, EPIC strongly opposes the sharp increase in funding for TSA's surveillance programs proposed in the president's FY 2006 budget, and specifically opposes funding of the Office of Screening Coordination and Operations.

---

[46] DHS Budget, *supra* at 19.
[47] *Id*.
[48] Transportation Security Administration, Department of Homeland Security, *Draft Privacy Impact Statements (CAPPS II)*, April 17, 2003, July 29, 2003, and July 30, 2003, obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/profiling.html.

Thank you for your consideration of these issues.

Sincerely yours,

_____
Marc Rotenberg
Executive Director

_____
Marcia Hofmann
Director, Open Government Project

_____
Melissa Ngo
Staff Counsel

Enclosures