U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security

Privacy Office

June 29, 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009

Re: **DHS/OS/PRIV 07-90/Hofmann request**

Dear Ms. Hofmann:

Pursuant to the order of the court, this is our third partial release to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated October 20, 2006, for DHS records concerning Passenger Name Records (PNR) from May 30, 2006 to the present including:

1. Emails, letters, reports or other correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the US for prescreening purposes;
2. Emails, letters, statements, memoranda or other correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the undertakings;
3. Records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used, disclosed to other entities, or combined with information from other sources; and
4. Complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data from EU citizens.

In our December 15, 2006 letter, we advised you that we had determined multiple DHS components or offices may contain records responsive to your request. The DHS Office of the Executive Secretariat (ES), the DHS Office of Policy (PLCY), the DHS Privacy Office (PRIV), the DHS Office of Operations Coordination (OPS), the DHS Office of Intelligence and Analysis (OI&A), the DHS Office of the General Counsel (OGC), the Transportation Security Administration (TSA), and U.S. Customs and Border Protection (CBP) were queried for records responsive to your request.

Continued searches in PRIV produced an additional 7 documents consisting of 27 pages of records responsive to your request. Of those 7 documents, I have determined that 2 documents totaling 6 pages are releasable in their entirety, 2 documents totaling 11 pages are releasable in part, and 3 documents totaling 10 pages are exempt from disclosure in their entirety. The

withheld information, which will be noted on the Vaughn index when completed, consists of names, email addresses, drafts, recommendations, legal opinions, Law Enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, and 7(E) of the FOIA, 5 USC §§ 552 (b)(2), (b)(5), (b)(6), and (b)(7)(E).

FOIA Exemption 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative tracking. FOIA Exemption 2(high) protects information the disclosure of which would risk the circumvention of a statute or agency regulation. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information.

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. It applies to facts divulged by a client to his attorney, and encompasses any opinions given by an attorney to his client based upon, and thus reflecting, those facts, as well as communications between attorneys that reflect client-supplied information.

FOIA Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Weighed against the privacy interest of the individuals is the lack of public interest in the release of their personal information and the fact that the release adds no information about agency activities, which is the core purpose of the FOIA.

Finally, FOIA Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Our office continues to process your request. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-90/Hofmann request.** The DHS Privacy Office can be reached at 703-235-0790 or 1-866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 17 pages

b(6)

From: b(6)
Sent: Tuesday, August 08, 2006 10:51 AM
To: Rosenzweig, Paul;

b(6) ; Scardaville, Michael;

b(6) **Cc:** ; Baker, Stewart
Subject: RE: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT
Importance: High

For Policy,

Below are consolidated comments to NSC draft. Once you clear, we will send to NSC on classified system. For OGC and CBP, double check my consolidation.

==========

Page 1 - I

Page 2 -

Page 2 -

Page 3 -

Page 2 - I

b(5)

Page 3 -

Page 3

b(5)

Page 3 -

Page 4 –

Page 4

Page 5 –

Page 5 -

p. 6 -

Page 6 - In

Page 7

b(6)

DHS, Privacy Office
Tel.
Fax:
Email:

b(6)
b(2)

From: Rosenzweig, Paul
Sent: Tuesday, August 08, 2006 8:40 AM
To:

b(6)

[redacted] Scardaville, Michael; [redacted]
[redacted]
Cc: Baker, Stewart
Subject: RE: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT

b(6)

My quick comments. has lead for collecting:

Page 1 –

Page 1 –

b(5)

Page 4 –

Page 5 –

Page 7 –

Paul

(2)
b(6)

Paul Rosenzweig

From:
Sent: Tuesday, August 08, 2006 7:58 AM
To: Rosenzweig, Paul;

b(6)
b(6)

b(6)

; Scardaville, Michael;

Cc:
Subject: URGENT: DC DISCUSSION PAPER FOR IMMEDIATE COMMENT
Importance: High

PLEASE PROVIDE COMMENTS TO ATTACHED NSC DRAFT NLT 10:30 AM THIS MORNING. POLICY WILL CLEAR A COORDINATED DHS RESPONSE TO NSC THIS MORNING. SEE ESPECIALLY NSC QUESTION AT TOP OF P. 5.

b(2)
b(6)

DHS, Privacy Office
Tel.
Fax:
Email:

b(2)
b(6)

From: Rosenzweig, Paul
Sent: Friday, August 04, 2006 5:08 PM
To:
Cc:

b(6)

, Rosenzweig, Paul;

Scardaville, Michael;
Subject:

John

b(6)

Edited and cleared – pls push to via classified system

Answers to NSC questions

Pages 1-2

b(5)

Page 2

b(5)

b(5)

Page 3

Is "ICE" Immigration and Customs Enforcement? Yes.

Page 6

b(5)

Page 1

b(5)

Page 2

Page 3

Page 4

b(5)

Note also: CBP does have authority to pull PNR prior to 72 hours if it gets information that a person of specific concern may be traveling on the flight–it is required to use normal LE channels if "practicable".

Page 5

b(5)

Page 3

Paul Rosenzweig
Counselor to the Asst. Secy. (Policy Directorate) and
Acting Assistant Secretary for Policy Development
Dept. of Homeland Security
Washington, DC 20528
Ph:
E:

b(2)
b(6)

[b(2) b(6)]

From: Baker, Stewart [b(2) b(6)]
Sent: Saturday, September 30, 2006 6:23 PM
To: [b(2) b(6)] Rosenzweig, Paul; [b(2) b(6)]
Subject: PNR press points

[b(2)]

This is not for release but provides useful talking points and background on the PNR issue.

From: [b(2) b(6)]
Sent: Saturday, September 30, 2006 5:34 PM
To: Kent, Don; [b(6)] Myers, Julie L; Allen, Charles; Martinez-Fonts, Al; Hawley, Kip; [b(6)] Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; [b(6)], Bergman, Cynthia; [b(6)]
Cc: [b(6)]
Subject: FINAL PNR PAG

TALKING POINTS

- Secretary Chertoff has initialed a draft formal U.S. /EU agreement regarding the sharing of Passenger Name Record (PNR) data.
- As we await the final ratification of the draft agreement, we expect that planes will continue to fly uninterrupted and our national security will not be impeded.
- The proposal ensures the appropriate security information will be exchanged and counter-terrorism information collected by the department will be shared, as necessary with other federal counter-terrorism agencies.
- The draft agreement has now been returned to the European Union for its review and consideration.
- The United States has a legal and moral obligation to protect its borders, as we have a right to verify who it is admitting into the country. This department will use every legal authority at our disposal, including valuable PNR data, to secure the borders of our homeland and fulfill the trust that the American people have placed in us.
- It is should be made clear that DHS is not seeking additional PNR data elements. The total number of data elements remains constant at 34. This is the same data that was permitted to be shared under the previous agreement.
- PNR data is used for our shared goal of combating terrorism while respecting fundamental rights and freedoms, notably privacy. The level of privacy protection afforded American and EU citizens remains unchanged.

- Here in the United States and in Europe, we all have to be smart and thorough in scrutinizing people seeking to enter our territory – including those who may not be on watchlists but could mean to do us harm.

- This is really a question of timing. Much of the PNR information could be gathered from travelers when they arrive in the United States, or DHS could impose visa requirements soliciting this information, but this would seriously impede travel. The only way we can avoid such a scenario is to ask for the information electronically in advance of travel.

- We look forward to finalizing an agreement on this issue with our European allies, with whom we have a great relationship

QUESTION AND ANSWERS

Q. What is PNR and what is it used for?
A: Passenger Name Record (PNR) is the generic name given to records created by aircraft operators and can include a range of elements such as date of ticket reservation, date and place of ticket issue, payment details, passenger/travel agent contact details and travel itinerary. This is data that can be obtained from a passenger during an interview with US Customs and Border Protection officers upon arrival in the United States.

Per the Aviation Transportation Security Act (ATSA) DHS collects PNR information on travelers aboard flights bound for and departing from the U.S. Our current agreement with the EU reflects this U.S. statutory requirement, which strengthens aviation and border security, while also facilitating legitimate travel.

CBP uses PNR along with other information to conduct a risk assessment of each passenger in order to identify those that may pose a threat of terrorism and other serious crime. Access to this information is a foundational element of DHS's layered strategy for aviation and border security and also facilitates legitimate travel.

Q: Will air travel be interrupted between US and Europe?
A: The appropriate security information will continue to be exchanged. Planes will continue to fly uninterrupted and our national security will not be impeded.

Q: What is DHS looking for in long term agreement with EU on PNR?
A: The issue for the US comes down to the need to break stovepipes among counterterrorism and law enforcement agencies. Every nation has a legal and moral obligation to protect its borders, as it has a right to verify who it is admitting into the country. This department will simply not relinquish that sovereign right, and we will use every legal authority at our disposal. Limits should not be placed on the sharing of PNR data by CBP with other elements of the U.S. government; particularly within DHS and the Department of Justice for the investigation, analysis, and prevention of terrorism and other crimes.

Q: Who does DHS receive PNR data on?
A: DHS receives PNR data for all passengers flying to the United States.

Q: How long does DHS want to store PNR data for?
A: We would like to store PNR data for as long as it has potential relevance for law enforcement and terrorism prevention purposes. Because we know terror attacks can be in the planning stages for several years, we want to store the information for longer than the current 3.5 year agreement.

Q: When does DHS begin collecting PNR data? Do you want to get it earlier?
A: We begin collecting PNR data up to 72 hours before flights for preliminary targeting. We would like to be permitted access to PNR outside of the 72 hour mark when there is an indication that early access could assist in responding to a threat to a flight or set of flights bound for the United States.

Q: Will there be further negotiations?
A: We look forward to finalizing the draft agreement with our European allies, with whom we have a great relationship.

Q: How will DHS obtain PNR? How does this method affect privacy?
A: We have agreed to work towards a "push" system, which may be viewed as less of a privacy concern than the current "pull" model by many Europeans. This would mean that air carriers are feeding us info rather than getting it from carrier records. In implementing this model we are working with carriers and system providers to ensure all technical specifications meet DHS regulatory requirements.

Q. What is the difference between Advance Passenger Information System (APIS) and Passenger Name Record (PNR) data?
A: APIS data refers to passenger information that is collected from government-issued identity documents accepted for international travel. APIS data is most commonly collected from passports and much of this information is resident in the Machine Readable Zone. APIS data comprises data elements such as Full Name, Date of Birth, Travel Document Number, Country of Issuance, etc.

PNR is the generic name given to records created by aircraft operators or their authorized agents for each journey booked on behalf of any passenger. The data is used by operators for their own business and operational purposes. PNR data comprises a range of elements such as date of ticket reservation, date and place of ticket issue, passenger/travel agent contact details and travel itinerary.

Q: What has been done to address privacy concerns over PNR data sharing?
A: CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance with U.S. privacy law and the 2004 EU-U.S. agreement.. This is a recognizable achievement that involved implementation of state-of-the-art technology solutions for use by officers of CBP nation-wide, the establishment of detailed training programs and the implementation of new policy and procedural rules that are paired with sever penalties for misuses.

The EU is aware of these investments and has voiced its approval. On September 20 and 21, 2005, delegations from DHS and the European Commission performed the first Joint Review of the PNR Undertakings concerning PNR derived from flights between the US and the EU. Prior to the Joint Review, the DHS Privacy Office conducted an internal review of CBP policies, procedures and technical implementation related to the data covered by the Undertakings and found CBP in full compliance with representations made in the PNR agreement. Afterwards, the EU issued its own report, which came to the same conclusion. Both of these reports are publicly available on the internet. [NOTE – PRIV report is on the DHS website]

Q: Did the European Court of Justice rule that U.S. data privacy protection is inadequate?
A: The Court did not rule against the availability of PNR data, it did not determine that privacy was violated, nor did it take a view on the content of the agreement. Rather, the court found that the European Council relied upon an inapplicable legal authority for entering into the agreement.

Q: How will the PNR agreement affect the Pre-departure APIS Notice of Proposed Rulemaking?
A: APIS is merely an automated vehicle for the collection of information from government-issued

identity documents accepted for international travel. The Pre-departure APIS proposed changing the timeing for APIS information already being collected under the APIS Final Rule Published on April 7, 2005. Essentially, APIS is the same as a border officer swiping or visually examining a passport presented by a traveler. The Pre-departure APIS NPRM does not contain any PNR related requirements. Thus, this rulemaking is not affected by the EU's recent PNR ruling.

Press Information

Decision of the European Court of Justice
On PNR Data Privacy Agreement between the US and European Union

- The Court did not rule against the sharing of PNR data. Nor did it determine that privacy was violated, or take a view on the content of the PNR agreement. Rather, the court found that the sharing of PNR data is a law enforcement issue, so the European Commission did not have competence to negotiate the agreement with the U.S.
- There will be no disruption of transatlantic air traffic as a result of the agreement. The European Court of Justice has given the EU until September 30 to identify another legal basis for the PNR agreement. Until then planes will continue to fly and important security data will continue to flow as normal.
- This is a complex case and we are currently reviewing the decision carefully. We look forward to cooperating with our European counterparts as they work toward a solution.

Background

Passenger Name Record (PNR) is the generic name given to records created by aircraft operators or their authorised agents for each journey booked on behalf of any passenger. The data is used by operators for their own commercial and operational purposes. PNR data comprises a range of elements such as date of ticket reservation, date and place of ticket issue, payment details, passenger/travel agent contact details and travel itinerary.

PNR data provides law enforcement officials with a valuable source of data for risk assessment. PNR data is available beginning 72 hours before a plane's departure. DHS has worked closely with airlines to move expeditiously to a system which sends, or "pushes" the data to DHS Customs and Border Protection.

The U.S. and the EU signed a PNR Agreement in May 2004. The PNR agreement included a set of Undertakings outlining appropriate collection and handling of PNR data. A September 20-21, 2005 US-EU Joint Review of the Undertakings found DHS's Customs and Border Protection in compliance.

This court decision did not judge DHS's ability to protect private information. The decision states that the European Commission did not have the authority to enter into such an agreement with the US. The decision does not question the content of the agreement, just the process for entering into the agreement.

PNR data should not be confused with Advanced Passenger Information System (APIS) data. APIS is created when a passenger checks in for a flight, as well as for a flight's crew – it is designed to provide an exact record of who was on a particular flight. APIS data is currently provided to the destination country no later than 15 minutes ***after*** a plane's departure. APIS data has been shared between nations for over a decade.

Following is a brief summary of some of Customs and Border Protection's (CBP's) Undertakings to protect PNR data:

- CBP will collect 34 data elements from the PNR, though in most cases the amount of data available in a PNR record will be much less.

- PNR will be used by CBP strictly for purposes of preventing and combating terrorism and related crimes, other serious crimes, including organized crime, that are transnational in nature, and flight from warrants and custody for such crimes.

- CBP will only be able to collect additional information, such as credit card account transaction data, by going through established, lawful channels.

- CBP will not use certain "sensitive data" -- i.e. personal data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual--which CBP has identified in consultation with the European Commission. This includes meal preference data.

- CBP will delete PNR data not manually accessed after 3½ years.

- No other local, state, federal, or foreign agency would have direct electronic access to PNR data through CBP databases.

- CBP will record and audit all access to PNR information through its databases to guard against its unauthorized use. Unauthorized access to or disclosure of PNR data is subject to strict disciplinary action by CBP which may include termination of employment or criminal sanctions.

- CBP will provide notice to the public regarding the PNR requirement and issues associated with the use of PNR.

- CBP will seek to rectify incorrect data at the request of passengers.

- Complaints regarding the collection or handling of PNR data by CBP may be made to CBP directly or through a European citizen's Data Protection Authority. Such complaints, if unsatisfactorily resolved by CBP, may be appealed to the DHS Chief Privacy Officer. The DHS Chief Privacy Officer may include a summary of these complaints in a subsequent report to the U.S. Congress.

For More Information, Please see the following Websites:

(System down, but would list:

DHS PNR fact sheet
DHS Privacy Office Review

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Via Electronic Delivery

ATTN: Director General Jonathan Faull
European Commission
B-1049 BRUXELLES
Belgium

ATTN: Ms. Irma Ertman
Presidency of the Council of the
European Union
Ministry of Foreign Affairs
P.O Box 176, Laivastokatu 22
FIN-00161 Helsinki
Finland

Dear Jonathan and Irma:

This letter is intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS). For the purposes of this letter, DHS means the Bureau of Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components of DHS such as the Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency. We look forward to further reviewing these and other issues in the context of future discussions toward a comprehensive, reciprocal agreement based on common principles.

Sharing and Disclosure of PNR

The Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, on October 25, 2005 the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment.

Pursuant to Paragraph 35 of the Undertakings (which states that "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law" and allows DHS to "advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings"), the U.S. has now advised the EU that the implementation of the Information Sharing Environment required by the Act and the Executive Order described above may be impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30, 31, and 32.

In light of these developments and in accordance with what follows, the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of the U.S. government responsible for preventing or combating of terrorism and related crimes as set forth in Paragraph 3 of the Undertakings.

DHS will therefore facilitate the disclosure (without providing unconditional direct electronic access) of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the expiration of the Agreement.

Early Access Period for PNR

While Paragraph 14 limits the number of times PNR can be pulled, the provision puts no such restriction on the "pushing" of data to DHS. The push system is considered by the EU to be less intrusive from a data privacy perspective. The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on DHS by U.S. law. Therefore, it is understood that DHS will utilize a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, taking into account the economic impact upon air carriers.

In determining when the initial push of data is to occur, DHS has discretion to obtain PNR more than 72 hours prior to the departure of a flight so long as action is essential to combat an offense enumerated in Paragraph 3. Additionally, while there are instances in which the U.S. government may have specific information regarding a particular threat, in most instances the available intelligence is less definitive and may require the casting of a broader net to try and uncover both the nature of the threat and the persons involved. Paragraph 14 is therefore understood to permit access to PNR outside of the 72 hour mark when there is an indication that early access is likely to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with offenses described in Paragraph 3 of the Undertakings. In exercising this discretion, DHS will act judiciously and with proportionality.

DHS will move as soon as practicable to a push system for the transfer of PNR data in accordance with the Undertakings and will carry out no later than the end of 2006 the necessary tests for at least one system currently in development if DHS's technical requirements are satisfied by the design to be tested. Without derogating from the Undertakings and in order to avoid prejudging the possible future needs of the system any filters employed in a push system, and the design of the system itself must permit any PNR data in the airline reservation or departure control systems to be pushed to DHS in exceptional circumstances where augmented disclosure is strictly necessary to address a threat to the vital interests of the data subject or other persons.

Data Retention

Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The Agreement will have expired before Paragraph 15 of the Undertakings requires the destruction of any data, and questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions.

The Joint Review

Given the extensive joint analysis of the Undertakings conducted in September 2005 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement.

Data Elements

The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3.

With this letter the U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding DHS's need to obtain the frequent flier number and any data element listed in Attachment A to the Undertakings wherever that element may be found.

Vital Interests of the Data Subject or Others

Recognizing the potential importance of PNR data in the context of infectious disease and other risks to passengers, DHS reconfirms that access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings. "Vital interests" encompasses circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay. Such data will be protected in a manner commensurate with its nature and used strictly for the purposes for which it was accessed.

Sincerely yours,

Stewart Baker
Assistant Secretary for Policy