Questions for the Record, Submitted by Senator Ron Wyden
Oversight Hearing on Transportation Security, September 9, 2003

Questions for Admiral James M. Loy:

On August 1, 2003, the Transportation Security Administration's (TSA) published a Federal Register Notice (68 Fed. Reg. 45265) concerning its plans to develop and implement a new version of the Computer Assisted Passenger Prescreening System, commonly known as "CAPPS II." I believe that this Notice was a positive first step in explaining to the public TSA's plans for CAPPS II, and in providing information needed to assess the program's potential impact on privacy. However, the Notice also left me with a number of questions as to how CAPPS II would operate. I believe that the answers to these questions are crucial to understanding the nature and implications of the system TSA is proposing. My questions fall into six main areas.

1. What Goes On in the "Risk Assessment" Portion of the Process

According to the explanation contained in the August 1 Federal Register Notice, CAPPS II will involve two main steps. The first step is authentication, in which the system will compare PNR data with data contained in commercial databases "for the sole purpose of authenticating passenger identity." The result will be a numeric score showing the confidence level that the identity the passenger provided is accurate.

The second step is the risk assessment. This is an area where I believe the explanations to date have been insufficient, making clarification essential.

1.a. The Federal Register Notice states that "[t]he risk assessment function is conducted internally within the U.S. government." Does this mean that, for purposes of the risk assessment, CAPPS II will not in any way query or otherwise make use of commercial databases?

1.b. If the risk assessment process does not involve making additional queries of commercial databases, then what information does it rely on? At a minimum, it appears that the risk assessment will involve checking to see if the passenger is on any federal list of known or suspected terrorists, or persons with outstanding arrest warrants for violent crimes. But are there additional sources of information, inside or outside government, that the risk assessment will use? Or does the risk assessment simply produce a "yes or no" answer as to whether the passenger is already on a government list of persons considered dangerous?

1.c. Checking against existing government watch lists seems like a straightforward way of determining whether a passenger is already known as a terrorist or suspected terrorist. But according to the Federal Register Notice, the risk assessment process will do more than that – it will determine the likelihood that the passenger has "identifiable links" to known terrorists or terrorist organizations. How can the risk assessment process ferret out such links, if the information it relies on consists of existing government watch lists? Is it envisioned that the

government will compile lists of all persons who have any link with a known terrorist or terrorist organization? Wouldn't this be an exceedingly broad list?

1.d. For example, suppose that a passenger once shared an apartment or college dorm room with a person who is now on a U.S. list of known terrorists. Would the risk assessment capture this link? If so, how? Would the risk assessment process check commercial databases, which may contain records of the passenger's past addresses? Or is it envisioned that this passenger would already be on a government watch list, based on this solely on this possibly innocent link?

1.e. The Federal Register Notice says that CAPPS II will generate a "risk score" for each traveling passenger. Is this "risk score" the product solely of the risk assessment process, or does it does it take into account the results of the authentication step as well? If the latter, does it factor in any data or information from the authentication process other than the numeric authentication score?

1.f. Suppose a passenger is not on a government watch list of known or suspected terrorists. Could the CAPPS II system nonetheless produce a high enough "risk score" to bar the passenger from flying?

2. Process for Detecting and Correcting Mistakes

The Federal Register Notice states that a passenger will be able to request access to the PNR data CAPPS II contains on him/her, and to request the modification of that data if the passenger believes it is inaccurate. However, the Notice goes on to observe that because CAPPS II will not retain data on passengers for any significant time, in most cases there will be nothing for the passenger to obtain or correct.

2.a. This suggests that, while a procedure for accessing and requesting modifications to records may be important in other contexts, this approach really isn't very useful for addressing mistakes that may occur under CAPPS II. Does TSA agree that CAPPS II is going to require other types of redress procedures?

2.b. For example, if the system repeatedly flags a particular individual as suspicious, what options will that individual have to rectify the problem? Suppose the problem stems from inaccurate information in a commercial database, which results in a low authentication score for that individual. In such a case, accessing records held by the CAPPS II system would be useless. How will the system deal with mistakes of this kind?

2.c. What is the justification for exempting CAPPS II from the Privacy Act's data access and correction requirements?

3. Accuracy of the "Identity Authentication" Part of the Process

The Federal Register Notice states that "[o]ne of TSA's primary purposes in creating this new system is to avoid the kind of miscommunication and improper identification that has, on

occasion, occurred under the systems currently in use. During the test period, TSA hopes to confirm that the use of the CAPPS II program will significantly reduce improper identification."

However, a recent Associated Press article ("Feds Don't Track Airline Watchlist Mishaps," by David Kravets, July 23, 2003) reported that TSA does not keep information on the number of people who are misidentified and wrongly delayed or barred from flights under the current system.

3.a. Does TSA have any systematic way of tracking how often the current system makes mistakes?

3.b. If not, how will TSA determine whether and to what extent CAPPS II will reduce the number of cases of mistaken identity?

3.c. To what extent will TSA make public the results of its testing on the accuracy of the identity authentication process? Will the public be permitted to see the numbers behind any claimed decrease in misidentification – and to evaluate the rate at which mistakes still occur under the new system?

4. Financial and Health Data

The Federal Register Notice states that the CAPPS II system "will not use measures of creditworthiness, such as FICO scores, and individual health records." However, this statement appears in the explanatory "Supplementary Information" section of the Notice. In what appears to be the official portion of the Notice – the part headed "DHS/TSA 010" – there is no reference to such a limitation.

4.a. What is the legal effect of the statement in the "Supplementary Information" section that CAPPS II will not use individual financial and health information?

4.b. Why is there no comparable statement in the body of the official Privacy Notice itself?

4.c. The Notice makes the CAPPS II system "exempt from publishing the categories of sources of records." Why is TSA claiming this exemption? As a legal matter, wouldn't this permit TSA, a year or two down the road, to reverse its decision to refrain from using individual financial and medical data – and to start using such data without telling the public? How can the public rely on any current TSA description of what information the CAPPS II system will or will not use, if TSA is reserving the right to expand or modify the information it uses without any public notice or scrutiny?

5. Procedures for Future Changes to CAPPS II

As noted above, the Notice makes CAPPS II "exempt from publishing the categories of sources of records." It also gives the CAPPS II system a security classification of "classified, sensitive."

Given this classified status and the exemptions from the Privacy Act, could TSA modify significant aspects of the CAPPS II program without disclosing the changes to the public? To what extent would TSA have the ability, from a legal perspective, to depart from the CAPPS II system description set forth in the Notice? Could a future TSA elect to make changes regarding the scope or operational characteristics of the CAPPS II system -- and do so secretly, without a formal and public regulatory process? How easily could the various representations and assurances made in the Notice be withdrawn?

6. Intended Future Link to Immigration Data

The Federal Register Notice states that "[i]t is . . . anticipated that CAPPS II will be linked with the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program at such time as both programs become fully operational, in order that processes at both border and airport points of entry and exit are consistent."

6.a. If the sole mission of the CAPPS II system is to determine whether a passenger may pose a risk to aviation security, why does the system need to be linked with immigration data? Is it anticipated that CAPPS II may eventually be used not only for safeguarding aviation security, but also for enforcing immigration law – for example, for apprehending illegal aliens or visitors who have overstayed their visas?

6.b. What are the specific "processes at both border and airport points of entry and exit" to which the Notice refers? What are the specific types of potential inconsistencies that TSA hopes to avoid by linking the CAPPS II and US-VISIT systems? Please provide some concrete examples of problems that could arise if the two systems were not linked.