DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

STATEMENT OF

DAVID M. STONE
ACTING ADMINISTRATOR

ON
THE SECOND GENERATION COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM
(CAPPS II)

BEFORE THE
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON AVIATION
UNITED STATES HOUSE OF REPRESENTATIVES

March 17, 2004

Good morning Mr. Chairman, Congressman DeFazio, and Members of the Subcommittee. I am pleased to have this opportunity to appear before you today on behalf of the Transportation Security Administration (TSA) to discuss the status of the Second Generation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). The Department of Homeland Security (DHS) and TSA firmly believe that development of CAPPS II is a vital ring in our system of systems approach to aviation security and we are working to quickly resolve remaining policy and privacy concerns in order to proceed with testing. The description in this testimony is the current vision of how CAPPS II will work.

As part of the Aviation and Transportation Security Act (ATSA) (P.L. 107-71), Congress directed that the Secretary of Transportation ensure that "the Computer-Assisted Passenger Prescreening System, or any successor system – is used to evaluate all passengers before they board an aircraft; and includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened." [1] This requirement became part of the mission of TSA, with overall responsibility transferring with TSA to DHS on March 1, 2003, as provided for in the Homeland Security Act of 2002.

Before discussing CAPPS II, and the vital impact it will have on aviation security, it is important to discuss the limitations of the current first generation passenger prescreening system – CAPPS. This system was jointly developed in the mid 1990s. It is operated by the airlines, not the Federal Government, and according to the industry, costs approximately $150 million per year to operate. CAPPS does not use a centralized

[1] ATSA, §136, amending 49 U.S.C. §44903.

structure; rather, each air carrier determines how best it can prescreen passengers under CAPPS. In some cases air carriers are able to electronically prescreen the passengers through their information technology system. In other cases, however, an air carrier must use paper lists of passengers who must be flagged for further security screening. This is too costly, time consuming, and error prone a method of prescreening passengers, especially in the wake of the 9/11 attacks on this country.

The rules CAPPS uses to select passengers for enhanced screening do not reflect today's threats to aviation. They flag large numbers of airline passengers because of innocent ticket purchase habits. These passengers then require enhanced screening, even though they may pose no discernible threat to aviation security. This is frustrating to passengers, and forces TSA to allocate resources to conduct extensive screening of a population that does not require it.

I am sure that the Members of this Subcommittee know full well that air carrier passengers complain that travelers who do not appear to pose a threat to aviation security are nevertheless selected for enhanced screening. TSA is also fully aware of these complaints. We also hear complaints from passengers who are incorrectly identified as being on government watch lists and recognize that these people must go through a time consuming and frustrating process to differentiate themselves from those individuals who are properly on the lists.

The reality of the situation, however, is that every day about 1.8 million passengers present themselves at airport security checkpoints and must be screened, yet the current CAPPS program provides little information on who these 1.8 million passengers are or whether they pose any threat to aviation security. As a result, TSA must perform additional screening to provide the level of security that we and the American public demand. That is in large part why we are developing CAPPS II, which includes a critical identity authentication component.

Because the first generation of CAPPS does not do enough to enhance aviation security, and because Congress directed, in ATSA, that any successor system must evaluate all passengers before they board an aircraft, TSA is working diligently to develop CAPPS II. This second generation prescreening system will be a centralized, automated, threat-based, real time, risk assessment platform. It will increase our ability to ensure the people are designated for secondary screening by using best practice identity authentication procedures combined with a risk assessment. A final aspect of prescreening being considered for CAPPS II, which I will discuss later, involves detecting individuals who are the subject of an outstanding Federal or state warrants for violent crimes.

CAPPS II is being designed to take the burden of operating the current CAPPS system from the airlines and will centralize all commercial verification and government data sharing and analyses under government control. This will allow CAPPS II to move beyond the current rules based system that uses only limited passenger itinerary information to determine screening level. CAPPS II is expected to employ technology

and data analysis techniques to conduct an information-based, identity authentication for each passenger using commercial information along with data each passenger provides to the airline upon making a reservation, along with information resident in airline reservation systems. CAPPS II will combine the results (scores) from the identity authentication with a risk assessment. Unlike the existing CAPPS system, CAPPS II will have built-in auditing capabilities and privacy protections, and will include a redress mechanism for passengers who believe that they have been incorrectly selected for additional screening or, in rare cases, misidentified as a threat. As currently designed, the entire process of vetting a passenger through CAPPS II should take a short amount time to accomplish, measured in seconds.

Currently, the CAPPS II system is being designed to perform the following functions:

- Obtain available Passenger Name Record (PNR) data from airlines and computer reservation systems. At a minimum this data will include full name, home address, home telephone number, and date of birth;

- Authenticate each passenger's identity using commercial companies providing authentication services. Specifically, commercial data aggregators will perform an identity authentication for each passenger using techniques traditionally applied to validate identity. The data aggregators will provide to CAPPS II a score reflecting the degree of certainty that the passengers are who they say they are. These commercial data aggregators will be prohibited by contract from using the PNR data obtained through the CAPPS II process for any other purpose, including commercial or marketing uses and they will not transmit to the government any of the public source information they will use to authenticate a passenger's identity. Compliance will be audited and enforced in real time by a National Security Agency (NSA) certified data guard that will permit monitoring use of such data and enable actions to be taken in response to any infringements;

- Compare the passenger identity information against the Terrorist Screening Center's consolidated terrorist screening database, and against lists of individuals who are the subject of outstanding warrants for violent criminal behavior maintained by U.S. Government data sources;

- Assess other risks based on current terrorist-related threat information;

- Disseminate the threat results to the appropriate airport screening or airport law enforcement authorities with sufficient advance notice (approximately 72 hours before flight takeoff, and again in the event of a last-minute ticket purchase or any passenger-initiated change in itinerary) in order to allocate necessary response resources. Initially, results will be sent to the airline reservation systems for encoding on the passenger's boarding pass; and

- Distribute to screening staff through code on boarding passes the necessary screening level for each passenger.

The possible categories of screening are as follows[2]:

- *Low risk*: passenger boards after routine screening;
- *Elevated or unknown risk*: the passenger will be subject to additional security screening prior to boarding (in overseas locations, TSA will need to work with appropriate officials in the host country to ensure additional security screening is conducted in accordance with that country's laws and screening procedures); and
- *Specific identifiable terrorist threat*: TSA will alert appropriate law enforcement authorities.

As stated earlier, our current modeling suggests that CAPPS II will result in substantially fewer passengers falling into the category of "elevated or unknown risk." Furthermore, we expect that annually no more than a handful of passengers will fall into the category of a "specific identifiable terrorist threat" that will require TSA to notify Federal, state, or local law enforcement agencies. Again, this number is far fewer than those that are brought to the attention of law enforcement agencies under the current airline operated prescreening system.

Unfortunately, there is a tremendous amount of misunderstanding regarding the development of CAPPS II. Certainly, in a democratic society, we should engage in a healthy debate about an individual's right to privacy and the right of the polity to protect itself and its citizens from acts of terrorism. But in order for this debate to be joined, it is necessary to fully understand the facts.

CAPPS II will not be an intelligence gathering system. CAPPS II will not be a data mining system. CAPPS II will not discriminate against individuals because of their race, religion, ethnicity, physical appearance, or economic strata. Individuals who have issues of credit worthiness will not be flagged for enhanced screening, or denied boarding. The key issues for prescreening are simply identity authentication – making sure passengers are who they say they are – augmented by intelligence information that can help us focus screening efforts.

We are designing CAPPS II so it will not maintain data files on passengers beyond the time necessary to complete their itineraries. CAPPS II will not access or contain records of credit card purchases made by passengers (although a passenger's credit card number may appear in airline booking information transmitted to the system) nor will it access or obtain information concerning what medicines passengers may buy, where they shop, or their lifestyles. The only information passed through the CAPPS II firewall from commercial data aggregators will be a generic score indicating confidence in the passenger's identity. This information is far less detailed than the information these same data aggregators provide in the commercial marketplace.

[2] Some passengers may also be selected for additional security screening based on random selection.

The privacy rights of individuals will be fully respected. TSA is working closely with the DHS Privacy Officer to ensure that this occurs. We have issued two Interim Privacy Act notices to date.[3] DHS has committed to issuing a Final Notice before the system becomes operational. This Final Notice will further refine the parameters on the use and retention of passenger data. As required by the E-Government Act of 2002 (P.L. 107-347), we will conduct and publish a Privacy Impact Assessment before the system becomes operational. We will also provide adequate notice to future passengers as required by the Privacy Act. This process will explain to passengers how their information is being used (subject to the requirements of national security) and what rights they have to complain or to seek a remedy. Current plans call for layered notices, beginning with publication in the Federal Register and on the DHS/TSA Web site. Because passenger information will be collected at the point of reservation, TSA will also work with the airlines and reservation agents to generate ideas for providing and documenting this important notice.

We will fully implement safeguards and protocols to ensure that no data gathered as part of a CAPPS II assessment will be made available for any commercial purposes, nor breached by computer hackers, nor subject to improper use by either Government or contractor employees. I would like to describe in detail some of these measures we are planning to take.

The CAPPS II system itself will be secure, and it will only be accessible to persons who require access for the performance of their duties as Federal employees or contractors to the Federal government. The guiding principle for access will be "need-to-know." Access will be compartmentalized, thus allowing access to persons based only on their individual need-to-know and only to the extent of their authorization (*e.g.*, a person might be permitted to access information with regard to the unclassified portion of the system, but be denied access to classified areas). A 24-hour audit trail will be used to monitor all persons accessing or attempting to access the system and will help to ensure compliance with access rules. Because the CAPPS II system will be entirely electronic, the audit trail will immediately and accurately document which individuals have had access to what information in the system.

TSA will take a multi-dimensional approach to safeguarding passenger data. The information is proactively protected in the network, the system, the application, and the monitoring of the system. Key components will be certified by the National Information Assurance Partnership to ensure that they adhere to a security rubric defined by the U.S.-sponsored, international Common Criteria for Information Technology Security Evaluation. Additionally, at the site where CAPPS II processing occurs, numerous operational, physical, and technical controls will ensure that only authorized individuals or systems may connect to the CAPPS II infrastructure. Each piece of the architecture operates in concert with the others to create a robust information assurance program.

We expect the data communications network to be a fundamental building block for the exchange of data between airlines and the CAPPS II system. Therefore, it is critical to

[3] January 15, 2003 and August 1, 2003.

note that the infrastructure will be a private, dedicated network. Thus, it will not be directly accessible via public networks, such as the Internet. Moreover, the network will employ multiple information assurance features to ensure the confidentiality, integrity, and availability of data exchange. Data exchange will be protected end-to-end through encryption between the CAPPS II system and the intended, designated airline or security screening end-point. Encryption will ensure that data cannot be reviewed, modified, or removed while in transit. Additionally, as data is received by the CAPPS II infrastructure, it will pass through a multi-tiered firewall to prevent unauthorized access to the system.

The systems upon which the CAPPS II applications will run form another of the security building blocks. During the commissioning of each system, a thorough information assurance evaluation will be undertaken. As part of this activity, systems will be "hardened," addressing known vulnerabilities and establishing a rigorous security posture. Each of the systems will be protected through the use of specialized security software designed to identify and respond to unexpected or unauthorized changes in the operating environment. Regular review of system audit records will ensure that potential problems are addressed and corrected expeditiously. Finally, proactive testing of the systems, so called "white-hat hacking," will keep the CAPPS II system's security posture constantly under internal review.

We will ensure that the applications that form the CAPPS II system safeguard information through arbitration of access control. This arbitration is based primarily on the application's ability to authenticate entities and processes. Every interaction within the CAPPS II system, from the receipt of data through processing and response, will require the subcomponents of the system to authenticate with one another. Additionally, in the case of remote entities, such as airlines, the system will be able to authenticate using digital certificates, a widely-used, robust form of verification. By using digital certificates, the CAPPS II applications will be able to interact with trusted, known entities. Additionally, data may be encrypted within the CAPPS II system to prevent the unauthorized release of any PNR data.

The final safeguarding component, the monitoring system, will view CAPPS II in a more holistic manner. Correlating information from the network, the systems, and the applications, the monitoring system will constantly generate a picture of the overall security posture of the system. Augmented by the use of Intrusion Detection sensors on the network and in the systems, the monitoring system will form a risk management platform that alerts CAPPS II staff to anomalous or troublesome events across the system. The clear benefit of this component is an ability to quickly identify a series of seemingly unrelated events which taken separately are no cause for alarm, but taken on the whole, warrant an investigation and corrective action.

In response to privacy concerns, CAPPS II will only retain passenger information for U.S. persons for a short period after the completion of a passenger's flight itinerary – currently estimated at between 72 hours and one week. After that period has passed,

there will be no information that CAPPS II can easily access in a useable format related to individual passengers, should there be a desire to do so.

We are designing a redress process that will allow passengers to submit complaints to TSA regarding CAPPS II. An essential part of the redress process is the establishment of the CAPPS II Passenger Advocate. The Passenger Advocate will focus on assisting passengers who feel that they have been incorrectly or consistently prescreened. When a passenger submits a complaint, and provides the Government with permission to observe and monitor the results of prescreening during the complainant's future flights, TSA will work with other government agencies and commercial data providers to analyze the results of prescreening. This analysis will determine if the complaint is related to prescreening or due to another part of the screening process (*e.g.*, random selection) and determine if selection by CAPPS II is related to data that may be appropriately corrected. Passengers will be afforded the opportunity to appeal these results to TSA HQ and then, in turn, to the DHS Privacy Office.

An important benefit of CAPPS II's identification authentication function can provide is to reduce greatly the number of passengers who are incorrectly identified as being on a U.S. Government terrorist watch-list. In addition, CAPPS II will use the consolidated terrorist screening database that TSC is currently implementing. Under the terms of the Memorandum of Understanding establishing the TSC, signed by the Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, the TSC is also developing quality control measures to further ensure the integrity, accuracy, and currency of data in its consolidated terrorist screening database. We all remember when travelers named "David Nelson" had difficulty at airline check-in because another person with that same name was on a watchlist. With the ability to authenticate the identification of most passengers, and with the improved system and procedures the TSC is implementing, we expect CAPPS II will greatly reduce the number of these "false positives."

TSA plans to test CAPPS II prior to its deployment to demonstrate its effectiveness, and to refine the operations and the redress mechanisms we are building. To date, individual airlines are reluctant to provide the Government with the necessary PNR information to enable us to test the system due to both public concerns over privacy questions and legal considerations. We understand these concerns, and are working on alternative solutions that may help us obtain limited data for testing. We are committed to providing the same degree of privacy protection for any test or full system PNR data use. Additional work in this area remains to be done before such an order or regulation would be issued, and we will keep this Subcommittee apprised of our progress.

The recent GAO report, released on February 13, 2004, responded to requirements set forth in the Homeland Security Appropriations Act, 2004 (P.L. 108-90). GAO generally concluded that in most areas that Congress asked them to review, our work on CAPPS II is not yet complete. DHS has generally concurred in GAO's findings, which in our view confirm that CAPPS II is a program still under development. As discussed earlier, the reluctance of air carriers and passenger reservation systems to provide TSA with critical

PNR data, and ongoing but unresolved discussions with organizations like the European Union (discussed below), have hampered our ability to move forward with the necessary testing. As we resolve the issues of access to PNR data, and the testing phase moves forward and results in a more mature system, we are confident we will be able to satisfy the questions Congress posed.

The GAO report did however fail to note that, notwithstanding the inability of TSA to test the system with PNR data, we have made substantial progress in development. CAPPS II has a baseline functioning system that has been tested using simulated PNR data from volunteer employees. Presently, CAPPS II modules can receive simulated PNR data through the Airline Data Interface (ADI), standardize and format the data, and transmit the formatted data through the identity authentication process. Further, CAPPS II is capable of conducting a basic risk assessment and receiving an authentication score. It has undergone integration testing to ensure that the modules can work together. Additional testing phases will verify that the system is functional, that it can process the large volume of air travelers, meet a desired turnaround time, and produce a risk assessment, resulting in a recommended screening level for each passenger.

We have also received significant cooperation from foreign governments who have embraced the concept of a robust passenger prescreening system. We are engaged in intensive discussions with the European Union (EU) regarding the delivery of PNR data from citizens covered by the EU. The members of the EU are very sensitive to the privacy concerns of their citizens, and we share their concerns. However, as continually demonstrated by threats against commercial airlines from certain international locations, we must collectively find a solution. The continual cancellation of certain flights of interest is one method of handling these threats. More effective prescreening of passengers is another, far less costly way.

There has been continuing concern about expanding "the mission" of CAPPS II -- that is, using the system in areas for which it was never intended. I earlier mentioned using CAPPS II to identify travelers with outstanding warrants for violent criminal behavior. Our Interim Privacy Act Notice, published in August 2003, made it clear that we would consider the ability of CAPPS II to identify individuals with outstanding warrants for federal or state crimes of violence. We believe that it is entirely appropriate to bring such individuals to the attention of law enforcement officers. A person fleeing from justice for a violent crime should not be able to use the aviation system to escape from justice. Again, this is an area where misinformation abounds. A passenger with unpaid parking tickets or an outstanding civil judgment is not a person subject to an outstanding warrant for a violent crime. Nor would this component of a CAPPS II assessment prevent air travel by people who have paid their debts to society. Nevertheless, our design work continues to clarify and narrow the amount of information collected, how the information may be used, the length of time the information may be retained, and the parties with whom information may be shared. Any and all changes will be published in the Final Privacy Act Notice.

Another area of concern revolves around the growing area of identity theft. Many have asked whether an individual who has stolen another person's identification can thwart CAPPS II by posing as the innocent victim. To answer this question, it is important to point out that because one of the primary functions of CAPPS II is to verify the identities of air travelers. Passengers making airline reservations must provide information that matches information contained in commercial databases. Frequently, those who commit identity theft change such information (*i.e.* home telephone number or home address), in order to perpetrate the fraud, receive credit cards that the victim never applied for, and avoid detection. The sophisticated methodologies used by the commercial sector that we are working to harness with the CAPPS II system are very likely to flag this anomaly. As we move toward testing CAPPS II with real PNR data, we will have a much better view of how well CAPPS II discerns legitimate travelers from those who have stolen an innocent person's identity, and seek to travel on commercial aircraft.

Mr. Chairman, CAPPS II remains a high priority for TSA, and we believe it will be an essential element of aviation security. We appreciate the support that you have voiced for quick implementation of CAPPS II. However, we are also much aware of the privacy concerns of many American citizens and our foreign counterparts, and the need to adequately educate the American public and others concerned about what CAPPS II will do and what it will not do. We are heavily engaged in resolving these concerns and look forward to your continued support and that of the Congress.

I will be pleased to answer any questions that you may have.