Transportation Security Administration

Security Threat Assessment for Aircraft Operators and Heliport Operators and their Employees that Conduct Air Tour Operations in New York City

August 16, 2004

Contact Point:

Lisa S. Dean
Privacy Officer
Transportation Security Administration
571.227.3947

Reviewing Official:

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security
202.772.9848

I. Introduction

Under the Aviation and Transportation Security Act (ATSA) and authority delegated from the Secretary of Homeland Security, the Assistant Secretary of Homeland Security for Transportation Security Administration (TSA) has "the responsibility for security in all modes of transportation…."[1] Among the TSA specific powers are the authorities under 49 U.S.C. § 114(f) to:

1. Receive, assess, and distribute intelligence information related to transportation security;
2. Assess threats to transportation;
3. Develop policies, strategies, and plans for dealing with threats to transportation;
4. Oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities; …[and]
5. Carry out such other duties, and exercise such other powers, relating to transportation security as the [Administrator] considers appropriate, to the extent authorized by law. [2]

These provisions grant the TSA broad authority to assess threats and threat information and to plan and execute such actions as may be appropriate to address such threats.

In response to specific intelligence information, the United States Government has raised the Homeland Security Threat Advisory Level to Orange for the financial services sector in New York City, Northern New Jersey, and Washington, DC. Based on new and unusually specific threat information, the Department of Homeland Security (DHS) has determined that implementation of certain security measures are necessary for Air Tour Helicopter Operators and Heliports serving them in New York City. Among these measures is the completion of threat assessments for those individuals connected to these operations. Accordingly, TSA has issued security directives requiring Aircraft Operators that conduct Air Tour Operations in the New York City area and the operators of heliports that serve them submit to TSA certain identifying information for all employees (collectively "heliport workers"). TSA will conduct these security threat assessments by comparing the heliport workers' information against available law enforcement and terrorist related databases and records. DHS has limited these security threat assessments to heliport workers operating in the New York City area to narrowly focus these security operations to the current threat information. These security threat assessments are conducted under the authority of 49 U.S.C. §§ 114 and 44936.

This Privacy Impact Assessment (PIA), conducted pursuant to the E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003, is based on the current design of the program and the Privacy

[1] 49 U.S.C. § 114(d).

[2] *Id.* § 114(f)(1)-(3), (11), (15).

Act system of records notice, Transportation Workers Employment Investigation System (DHS/TSA 002), that was published in the Federal Register on August 18, 2003. This PIA provides further detail about the collection of personally identifiable information for the purpose of conducting the security threat assessments described above.

II. System Overview

- **What information will be collected and used for this security threat assessment?**

The following information is collected from Heliport Operators and Air Tour Operators for heliport worker security threat assessments: full name, aliases, date of birth, social security number, employer's name and upon request, fingerprints.

- **Why is the information being collected and who is affected by the collection of this data?**

The information is being collected in order to conduct security threat assessments on heliport workers involved in air tour helicopter operations in the New York City area. These security threat assessments are conducted under the authority of 49 U.S.C. §§ 114, 44901 and 44936. New York City Heliport Operators and Air Tour Operators and their employees are affected by this collection. TSA will also collect the names of New York City area air tour passengers to run against the "Selectee" and "No-Fly" lists.

Passenger Information

TSA will collect the names of New York City air tour passengers from Air Tour Operators to compare with those names that are contained in the "Selectee" and "No-Fly" lists. No information will be retained on passengers who are not matches to names contained on these two lists. Persons whose names appear on the "Selectee" list will not have their information retained, but will be subject to enhanced passenger screening of their persons and belongings. Persons whose names appear on the "No-Fly" list will not be permitted to board the aircraft. As appropriate, TSA will contact members of law enforcement and/or intelligence agencies and provide them with the passenger's name.

- **What information technology system(s) will be used for this program and how will they be integrated into a step-by-step process?**

TSA will conduct a security threat assessment on heliport workers consisting of two parts: a name based check and a criminal history records check (CHRC). The two phases of the security threat assessment are detailed below.

Name-based Check

Heliport Operators and Air Tour Operators will send their employees' full name, aliases, date of birth, social security number, and the employer's name to TSA via password protected e-mail. Upon receipt of this information, TSA will password protect this information to ensure only those with an operational need to know will have access to this personal data. TSA will send the

information via password-protected e-mail to American Association of Airport Executives (AAAE) for clearinghouse services that the association provides for TSA. AAAE currently provides clearinghouse functions for security threat assessments conducted in the aviation industry, including providing quality control procedures on the information and facilitating the transfer of it between TSA and the aviation industry. Using these services for these security threat assessments allows TSA to efficiently conduct the security threat assessment in a timely manner with a clearinghouse who already provides such services to TSA. AAAE will format all data received into one workable format for TSA. TSA will run this information through terrorist-related databases it maintains or uses. Any individual who meets the minimum criteria established by TSA as a possible match, will undergo further analysis. After TSA's review the name of any heliport worker who poses, or is suspected of posing, a security threat will be forwarded to appropriate intelligence and/or law enforcement agency(ies). The law enforcement or intelligence agency will analyze the information, determine whether the individual's identity can be verified and whether he or she continues to pose a threat or is suspected of posing a threat. If so, the law enforcement or intelligence agency will notify TSA of the determination so that TSA can inform Heliport Operators and Air Tour Operators that the individual worker is ineligible for access to the helicopter or to screened passengers and their accessible property. The law enforcement or intelligence agency will take appropriate action concerning the individual, depending on what information connects the individual to terrorist activity. TSA will use this procedure to ensure that any resulting information suggesting a connection between heliport workers and terrorist activities is as narrowly drawn as possible. TSA plans to continue conducting these security threat assessments indefinitely.

Fingerprint-based Check

In addition to the name based security threat assessment, throughout the course of conducting the security threat assessments, TSA may find circumstances warranting fingerprinting of heliport workers in order to facilitate a Criminal History Records Check (CHRC). Upon a request from TSA, Heliport Operators and Air Tour Helicopter Operators must have their employees submit a fingerprint application and fingerprints to TSA through the National Air Transportation Association (NATA), a TSA designated agent. NATA currently collects fingerprints for smaller air carriers and others in the aviation industry that do not already have fingerprinting capabilities at their airports. TSA will use NATA to collect fingerprints for the required CHRC because NATA already can provide this service efficiently and in a timely manner. Once the biometric information is collected, NATA sends it to AAAE. AAAE aggregates and conducts quality control of information and sends this information to TSA via secured email. TSA then transmits the information, including the fingerprint, to the FBI for a criminal history records check (CHRC). The FBI returns the results to TSA's Secure Fingerprint Results Distribution (FPRD) website, where TSA can access the information and adjudicate the results. The results are analyzed to determine if a worker has a disqualifying criminal offense pursuant to 49 CFR §§ 15 42.209 and 1544.229. Such offenses would render a heliport worker ineligible for access to the helicopter or to screened passengers and their accessible property. TSA will notify Heliport Operators and Air Tour Operators if an employee is determined to be ineligible for access to the helicopter or to screened passengers and their accessible property. Individuals will be given an opportunity to correct any underlying misidentification.

- **What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?**

TSA's security directive requires Heliport Operators and Air Tour Operators to provide employee identification information minimally sufficient to perform DHS name-based security threat assessments. It is expected that the information will typically not require an additional collection of information from any individual. TSA's system of records notice DHS/TSA 002, which was published in the Federal Register, provides public notice of the collection, use, and disclosure of this information. When TSA collects fingerprints through its agent, individuals will be provided with a Privacy Act notice pursuant to 5 U.S.C. § 552a of the Privacy Act of 1974 describing the authority to collect the information, the principal purpose for collecting the information, the routine uses which may be made of the information, and the effects, if any, of not providing all or any part of the requested information.

- **Does this program create a new system of records under the Privacy Act?**

No. This program is covered under a Privacy Act system of records that was established in 2003 called the "Transportation Workers Employment Investigation System," or DHS/TSA 002. The purpose of this system of records is to facilitate the performance of background investigations of transportation workers to ensure transportation security. The system of records notice was published in the Federal Register on August 18, 2003, and can be found at 68 Fed. Reg. 49496, 49498.

- **What is the intended use of the information collected?**

Information will be used for performing security threat assessments of heliport workers and to compare passenger names against those contained on the "No-Fly" and "Selectee" Lists.

- **With whom will the collected information be shared?**

The information will be shared with the appropriate DHS personnel and contractors with a "need to know," who, by law and contract are subject to the Privacy Act and who are involved in processing the security threat assessments. It will also be shared with the organizations referenced herein who will receive the information in order to format it for TSA's use. The information collected will also be shared with the FBI for purposes of conducting background checks. If persons pose or are suspected of posing a security threat, then TSA will notify the appropriate law enforcement and/or intelligence agency. The collection, maintenance, and disclosure of information will be conducted in compliance with the Privacy Act and the published system of records notice.

- **How will the information be secured against unauthorized use? (What technological mechanism will be used to ensure security against hackers or malicious intent?)**

TSA will secure personal information against unauthorized use through the use of a layered security approach involving procedural and information security safeguards. Specific privacy safeguards can be categorized by the following means, which are described in greater detail elsewhere in this document:

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

The Privacy Act of 1974, as amended, (5 USC 552a) which requires Federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of information protected by the Act.

Federal Information Security Management Act of 2002, (Public Law 107-347), which establishes minimum acceptable security practices for Federal computer systems.

- **Will the information be retained and if so, for what period of time?**

TSA intends to retain these records for a sufficient period of time to permit affected individuals an opportunity to pursue appropriate redress or appeal measures, as well as to permit TSA to retain adequate records of its actions under this program for auditing and other purposes. TSA does not yet have a record retention schedule approved by the National Archives and Records Administration (NARA) for records pertaining to this program. TSA is in the process of developing a records retention schedule that will dictate the retention period for these records. Once the records schedule is approved, TSA will amend this document to include the retention period for these records.

- **Will the information collected be used for any purpose other than the one intended?**

Information collected will be used to conduct security threat assessments for heliport workers. TSA ensures that this is accomplished through legal agreements with its contractors and agents and in compliance with the Privacy Act and the published system of records notice.

- **How will the Heliport Workers be able to seek redress?**

In the case of criminal history records checks (CHRC) resulting in a disqualifying offense, the individual may dispute the results of a CHRC (i.e., disposition of a charge (s) is incorrect); the worker can provide court documentation or other evidence to TSA. If the worker can show that the disposition (or charge) does not fall under the disqualifying offense category; he or she will be cleared for access to the helicopter or to screened passengers and their accessible property. If

the applicant can show that corrected disposition or charge no longer falls under the disqualifying offense category he or she will likewise be allowed such access.

Individuals who believe that they have been wrongly identified as a security threat will be given the opportunity to contact the Credentialing Program Office of TSA to address their concerns. Redress based on the security threat assessment (STA) will be handled on a case-by-case basis due to the classified and/or security sensitive information that may be involved. TSA will provide information on which the determination was based to the applicant to the extent permitted by law. There may be items that are classified or sensitive law enforcement and security information that TSA cannot release.

- **What technical safeguards are in place to secure the data?**

    - DHS employs the following technical safeguards to secure data: Secure data transmission, including the use of password-protected e-mail for sending files among the participants listed above, to prevent unauthorized internal and external access.

    - Password protection for files containing personal or security threat assessment data to prevent unauthorized internal and external access.

    - Network firewalls to prevent intrusion into DHS network and TSA databases.

    - User identification and password authentication to prevent access to security threat assessment systems by unauthorized users.

    - Security auditing tools to identify the source of failed TSA system access attempts by unauthorized users and the improper use of data by authorized operators.

Privacy Threats and Mitigation Measures

The table below provides an overview of the privacy risks associated with security threat assessments for air tour helicopter and heliport operator employees and the types of mitigation measures that address those risks.

Table 1: Overview of Privacy Threats and Mitigation Measures

Type of Threat	Description of Threat	Type of Measures to Counter/Mitigate Threat
Unintentional threats from insiders[3]	Unintentional threats include flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians (i.e., personnel of organizations with custody of the information). These threats can be physical (e.g., leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibilities.	These threats are addressed by (a) developing a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; developing, integrating, and configuring the system in accordance with those requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders	Threat actions can be characterized as improper use of authorized capabilities (e.g., browsing, removing information from trash) and circumvention of controls to take unauthorized actions (e.g., removing data from a workstation that has been not been shut off).	These threats are addressed by a combination of technical safeguards (e.g., access control, auditing, and anomaly detection) and administrative safeguards (e.g., procedures, training).

[3] Here, the term "insider" is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

Type of Threat	Description of Threat	Type of Measures to Counter/Mitigate Threat
Intentional and unintentional threats from authorized external entities	Intentional: Threat actions can be characterized as improper use of authorized capabilities (e.g., misuse of information) and circumvention of controls to take unauthorized actions (e.g., unauthorized access to systems). Unintentional: Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians	These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of routine use agreements which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program.
Intentional threats from external unauthorized entities	Threat actions can be characterized by mechanism: physical attack (e.g., theft of equipment), electronic attack (e.g., hacking, interception of communications), and personnel attack (e.g., social engineering).	These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards (e.g., identification and authentication, encrypted communications), and clear operating instructions and training for users and system administrators.

- **Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?**

All TSA and contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. Additionally, training will be conducted that relates to the handling of personal data specifically related to these security threat assessments. Staff assigned to handle classified threat assessment information will be required to obtain appropriate security clearances.

Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. Physical access safeguards include the use of armed or unarmed security guards at sites; hard-bolting or fastening of databases, servers, and workstations; and credential readers for internal and external site access. The DHS contractors also hold appropriate facility security clearances.

For questions or comments, please contact:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 202-772-9848