grade, minority status, and personnel transaction date. Investigative information consists of investigation targets' name and social security account number, organization name, type of investigation, offense data, source of referral data and action taken.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Inspector General Act of 1978, 5 U.S.C. App.

PURPOSES:

The purpose of the system is to provide individuals with a need to know with specific information related to (1) Time and attendance of employees; (2) workload status reports; (3) security clearance alerts; (4) travel information; and (5) investigation information. The Inspector General publishes some investigation results publicly through a public Web site, in combination with investigation results of other agencies and organizations, in an effort to coordinate fraud enforcement and investigation efforts with other entities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) Security clearance notification alerts may be provided to an examined activity in advance of visits by OIG personnel if information to be examined requires a secret clearance or above; (2) time and attendance reports will be used to track temporary duty travel frequency and duration, to categorize indirect time for periodic reports, and to accrue staff hour data on assigned projects; (3) planned annual leave reporting will be used by various managers for workload planning and travel scheduling; (4) assignments information and workload status information will be used by managers to control audits and investigations, and to maximize effectiveness of staff resources; (5) miscellaneous personnel information will be used by staff managers to determine training needs, promotional eligibility, education and background, and professional organization participation; (6) information will be used to produce resource management reports; (7) travel information will be used by managers to control temporary duty travel, travel costs and issuances of travel orders; and (8) investigative information is collected and maintained in the administration of the Inspector General Act of 1978 (Pub. L. 95–452) to investigate, prevent, and detect fraud and abuse in departmental programs and operations. Material gathered is used for investigative case management, and some investigation information is posted publicly in an effort to reduce fraud and other crimes across the government. See also Prefatory Statement of General Routine Uses.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Active reports on magnetic disk, with backup active records and inactive records maintained on magnetic tape.

RETRIEVABILITY:

Records will be retrievable through employee social security number, by name, or incident title, with selected records having certain secondary keys consisting of certain other data elements, listed in the ''Categories of Records in the System.''

SAFEGUARDS:

(1) Records will be maintained in a private library not accessible by any unauthorized user; (2) authorized user identification codes will be tied to multiple password system to afford additional protection; (3) any attempt to bypass the password protection system will result in ''Log-Off'' from the system or denial of access to data if access to system is authorized; (4) physical access to system documentation, hardcopy printouts, personal data files, and terminals will be restricted to authorized personnel by maintaining a secure environment in the headquarters office; and (5) tape files will be maintained in an environmentally secure vault area when not in use.

RETENTION AND DISPOSAL:

Records will be maintained for 2 years after they become inactive. All inactive records will be maintained on magnetic tape within the computer center and will be afforded the same safeguards as active records. Machine-resident records will be destroyed at the end of the 2-year period. Hard copy records will be retained until the records are replaced or become obsolete.

SYSTEM MANAGER AND ADDRESS:

Chief Information Officer, JM–10, Office of Inspector General, Department of Transportation, 400 7th Street, SW., Room 7117, Washington, DC 20590.

NOTIFICATION PROCEDURE:

Same as ''System Manager.''

RECORD ACCESS PROCEDURES:

Same as ''System Manager.''

CONTESTING RECORD PROCEDURES:

Same as ''System Manager.''

RECORD SOURCE CATEGORIES:

(1) Official personnel folder; (2) other personnel documents; (3) activity supervisors; (4) individual applications and forms; and (5) information obtained from interviews, review of records and other authorized investigative techniques.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Investigative data compiled for law enforcement purposes may be exempt from the access provisions pursuant to 5 U.S.C. 552a(j)(2), (k)(1), or (k)(2).

Dated: November 28, 2005.

Kara Spooner,

Departmental Privacy Officer.

[FR Doc. E5–7599 Filed 12–20–05; 8:45 am]

BILLING CODE 4910–62–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

First Meeting: RTCA Special Committee 207/Airport Security Access Control Systems

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of RTCA Special Committee 207 Meeting, Airport Security Access Control Systems.

SUMMARY: The FAA is issuing this notice to advise the public of a meeting of RTCA Special Committee 207, Airport Security Access Control Systems.

DATES: The meeting will be held January 18–19, 2006, from 9 a.m.–5 p.m.

ADDRESSES: The meeting will be held at RTCA, Inc., MacIntosh-NBAA & Hilton-ATA Rooms, 1828 L Street, NW., Suite 805, Washington, DC 20036.

FOR FURTHER INFORMATION CONTACT: (1) RTCA Secretariat, 1828 L Street, NW., Suite 805, Washington, DC 20036; telephone (202) 833–9339; fax (202) 833–9434; Web site *http://www.rtca.org.*

SUPPLEMENTARY INFORMATION: Pursuant to section 10(a)(2) of the Federal Advisory Committee Act (Pub. L. 92–463, 5 U.S.C., Appendix 2), notice is hereby given for a Special Committee 207 meeting. The agenda will include:

- January 18:
- Opening Plenary Session (Welcome, Introductions, and Administrative Remarks)
- Agenda Overview
- Workgroup Reports
- Workgroup 2
- Workgroup 3
- Workgroup 4
- Workgroup 5

- Workgroup 6
- Workgroup 7
- ICAO Update
- Discussions on vendor presentations—guidelines are as follows: The vendor/product categories sought are under Access Control, Perimeter Intrusion Detection, Biometric Systems/Devices, and Credentialing of employees. Each vendor seeking to present a short (maximum of 15 minutes) presentation to the committee members, will provide the briefing package, slides and supporting documents to Mr. Paul S. Ruwaldt (*paul.ruwaldt@dhs.gov* or *paul.s.ruwaldt@tc.faa.gov*) by January 4th, 2006, outlining the following:

• If the product is an access control system, sub-system or component of or could be applied to an airport access control system, the vendor is required to submit documentation, in written form, attesting to their understanding of the current DO–230A Airport Access Control Standard requirements and a description of how their product, system, sub-system or component complies with this current standard (this document will be inclusive of how their product(s) would be utilized in an automated access control system suitable for use under the requirements included in 49 CFR subpart 1500 et al.).

• How their product(s) would provide for (or enhance) the security objectives of the airport, and

• How their product(s) would be integrated into an airport comprehensive security system.

It is strongly suggested that the vendors requesting presentation time be fully cognizant of the airline and airport operational requirements as they apply to automated access control systems, perimeter intrusion detection, biometric system applications and credentialing application of employees, as well as the performance requirements of DO–230A and how their product(s) will interface, integrate or fuse (data) with automated access control systems. Further, it is suggested that the vendor by fully aware of how these operational and performance conditions will affect their product(s) and the access control procedures.

In addition, for those products or systems incorporating biometrics, specific reference and discussions will address the Biometric Guidance Package released and approved by the TSA this year.

The vendor presentation must strictly be pertinent to their product(s) and the relevant 49 CFR subpart 1500 et al. requirements for airport access control systems. The vendor must demonstrate their product's suitability to airline and airport operational access control conditions and illustrate how their product(s) would be deployed in automated access control systems and/or how their product(s) can be integrated into the automated access control systems.

The SC–207 committee emphasizes that this RTCA standard pertains only to airport access control systems, although there may be opportunities for future integration with other airport and federal information and/or communication technologies.

Further, the committee is interested in proven and available COTS technologies and/or products. The committee is not interested in yet untested, developmental concepts, representative products, systems or sub-systems or proprietary systems.

The vendors making presentations will be required to provide a soft copies of the material they wish to present to the committee. No material save that provided by the vendor by the 5th of January 2006 will be accepted or received by the Committee during the presentation on January 18th & 19th, 2006.

The presentations provided by the vendors will be collected and made available to the committee members in CD format on the day of the presentation.

It is expected that there will be only a limited presentation opportunity on these two days. Reservations will be made on a first come first served basis.

The Vendor should contact Mr. Ruwaldt via email to express interest in presenting. Once Mr. Ruwaldt receives the material, he will schedule the vendor's presentation time and date. All material must be received before this scheduling can take place.

If the presentation schedule is full for these two days, following consultation with the SC–207 Chairman, an additional presentation date in March could be allocated, however all vendors should not rely on this, and attempt to develop and provide their product(s) presentations as early as possible.

SC–207, in its deliberations for the updated standard DO–230B, is considering requiring that the products, systems, sub-systems and components utilized within airport access control systems, inclusive of perimeter, biometric intrusion detection and surveillance functions should be tested and verified to the requirements defined within the proposed DO–230B Standard.

Any such decision, including the identification of a responsible authority for conducting such verifications (or potential certification of products) will be taken before the final issuance of DO–230B.

- Closing Plenary Session (Other Business, Establish Agenda, Date and Place for Fourth, Fifth and Sixth Meeting).

Attendance is open to the interested public but limited to space availability. With the approval of the chairmen, members of the public may present oral statements at the meeting. Persons wishing to present statements or obtain information should contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section. Members of the public may present a written statement to the committee at any time.

Issued in Washington, DC, on December 14, 2005.

Natalie Ogletree,

FAA General Engineer, RTCA Advisory Committee.

[FR Doc. 05–24320 Filed 12–20–05; 8:45am]

BILLING CODE 4910–13–M

DEPARTMENT OF TRANSPORTATION

Federal Motor Carrier Safety Administration

[Docket No. FMCSA–2005–20930 (PDA–31(F))]

Notice of Delay in Processing the Application by American Trucking Associations, Inc. for a Preemption Determination Concerning the District of Columbia Restrictions Regarding Highway Routing of Certain Hazardous Materials

AGENCY: Federal Motor Carrier Safety Administration (FMCSA), DOT.

ACTION: Notice.

SUMMARY: In accordance with statutory requirements, FMCSA is publishing a notice of delay in processing the American Trucking Associations, Inc.'s (ATA) application for a preemption determination. FMCSA is conducting fact-finding in response to ATA's request, and is delaying issuance of its determination in order to allow time for appropriate consideration of the issues raised by ATA's application.

FOR FURTHER INFORMATION CONTACT: James Simmons, Chief, Hazardous Materials Division (MC–ECH), (202) 493–0496; Federal Motor Carrier Safety Administration, 400 Seventh Street, SW., Washington, DC 20590–0001. Office hours are from 7:45 a.m. to 4:15 p.m., ET, Monday through Friday, except Federal holidays.

SUPPLEMENTARY INFORMATION: ATA applied for an administrative determination that Federal hazardous